*Supplemento ordinario alla "Gazzetta Ufficiale" n. 275 del 26 novembre 2001 - Serie generale*

*Spediz. abb. post. 45% - art. 2, comma 20/b*
*Legge 23-12-1996, n. 662 - Filiale di Roma*

# GAZZETTA UFFICIALE
## DELLA REPUBBLICA ITALIANA

*PARTE PRIMA* **Roma - Lunedì, 26 novembre 2001** SI PUBBLICA TUTTI I GIORNI NON FESTIVI

DIREZIONE E REDAZIONE PRESSO IL MINISTERO DELLA GIUSTIZIA - UFFICIO PUBBLICAZIONE LEGGI E DECRETI - VIA ARENULA 70 - 00100 ROMA
AMMINISTRAZIONE PRESSO L'ISTITUTO POLIGRAFICO E ZECCA DELLO STATO - LIBRERIA DELLO STATO - PIAZZA G. VERDI 10 - 00100 ROMA - CENTRALINO 06 85081

**N. 250**



GARANTE PER LA PROTEZIONE
DEI DATI PERSONALI

# Provvedimenti concernenti il trasferimento di dati personali dal territorio dello Stato verso Paesi terzi.

# SOMMARIO

## GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

# DECRETI E DELIBERE DI ALTRE AUTORITÀ

## GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

DELIBERAZIONE 10 ottobre 2001.

**Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso Paesi non appartenenti all'Unione europea in conformità alle clausole contrattuali tipo di cui all'allegato alla decisione della Commissione europea del 15 giugno 2001, n. 2001/497/CE.** (Deliberazione n. 35).

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del Prof. Stefano Rodotà, presidente, del Prof. Giuseppe Santaniello, vice-presidente, del Prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 25 della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 secondo cui i dati personali possono essere trasferiti in un Paese non appartenente all'Unione europea qualora il Paese terzo garantisca un livello di protezione adeguato, nei termini previsti nel paragrafo 2 del medesimo articolo;

Visto l'art. 26 della predetta direttiva il quale individua alcune deroghe al menzionato principio, prevedendo anche che uno Stato membro possa autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un Paese terzo che non garantisce un livello di protezione adeguato, qualora il titolare del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi, risultanti anche da clausole contrattuali appropriate;

Visto il comma 4 del medesimo articolo 26 sulle decisioni della Commissione europea in materia di clausole contrattuali tipo;

Vista la decisione della Commissione europea del 15 giugno 2001 n. 2001/497/CE (pubblicata sulla *Gazzetta Ufficiale delle Comunità europee* L 181 del 4 luglio 2001) secondo la quale alcune clausole contrattuali tipo, allegate alla medesima decisione, costituiscono garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi, in caso di trasferimento di dati personali verso Paesi terzi a norma della direttiva 95/46/CE;

Considerato che gli Stati membri devono adottare le misure necessarie per conformarsi alla decisione della Commissione, ai sensi del paragrafo 4 del citato art. 26 della direttiva;

Visto l'art. 28 della legge 31 dicembre 1996, n. 675 secondo cui il trasferimento dei dati personali all'estero può avvenire: *a*) qualora l'ordinamento dello Stato di destinazione o di transito dei dati assicuri un livello di tutela delle persone adeguato o, se si tratta di dati sensibili o di taluni dati di carattere giudiziario, di grado pari a quello assicurato dall'ordinamento italiano; *b*) oppure, qualora ricorra uno dei casi previsti nel comma 4 del medesimo articolo; *c*) in ogni caso, qualora sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto (comma 4, lett. g));

Ritenuta la necessità di adottare, in conformità al citato art. 28, una misura necessaria per l'applicazione della decisione della Commissione;

Ritenuto che le citate clausole contrattuali tipo, che sono state articolate dalla Commissione in n. 11 clausole e n. 3 allegati anche sulla base del parere favorevole del Gruppo delle autorità garanti europee di cui all'art. 29 della citata direttiva, prevedono alcune garanzie per i diritti dell'interessato da ritenere adeguate ai sensi del citato art. 28, comma 4, lett. g);

Considerato che i soggetti che utilizzano le citate clausole contrattuali possono prevedere ulteriori garanzie per le persone cui si riferiscono i dati, rispetto alle garanzie minime previste dalle clausole medesime;

Rilevato che la decisione della Commissione riguarda unicamente i trasferimenti di dati effettuati a partire dal territorio dello Stato da un titolare del trattamento avente sede nella Comunità (soggetto esportatore) ad un diverso titolare del trattamento (soggetto importatore) e che un'ulteriore decisione della Commissione individuerà altre clausole contrattuali tipo per i trasferimenti di dati effettuati da un titolare del trattamento avente sede nella Comunità ad un responsabile del medesimo trattamento;

Ritenuta la necessità di assicurare ulteriore pubblicità alle predette clausole contrattuali tipo, disponendo la loro pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana in allegato alla presente autorizzazione;

Ritenuta la necessità di formulare nel dispositivo alcune precisazioni nell'esercizio dei compiti demandati a questa Autorità dall'art. 28 della citata direttiva e dalla legge n. 675/1996, richiamati anche dalla citata decisione della Commissione, nei limiti necessari per la prima fase di applicazione del presente provvedimento;

Ritenuto di dover riservare la scelta del Garante di svolgere o meno, caso per caso, il ruolo di mediazione previsto dalla clausola n. 7, paragrafo 1, lett. a) della Decisione;

Riservata la specificazione di ulteriori criteri e modalità in base all'esperienza maturata nell'utilizzazione delle clausole, anche in sede comunitaria;

Vista la documentazione d'ufficio;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il prof. Stefano Rodotà;

TUTTO CIO' PREMESSO IL GARANTE:

1) autorizza i trasferimenti di dati personali dal territorio dello Stato verso Paesi non appartenenti all'Unione europea, effettuati sulla base e in conformità alle clausole contrattuali tipo di cui all'allegato alla decisione della Commissione europea del 15 giugno 2001 n. 2001/497/CE, con effetto dal 3 settembre 2001 e sulla base dei seguenti presupposti:

a) il soggetto esportatore e il soggetto importatore devono richiamare o incorporare le clausole nei contratti relativi al trasferimento dei dati in modo da renderle riconoscibili anche alle persone cui si riferiscono i dati e che chiedano di averne conoscenza, evitando altresì la previsione di clausole limitative o incompatibili *(clausole nn. 4, lett. c) e 5, lett. e);considerando alla decisione n. 5);*

b) la copia del contratto relativo al trasferimento e le altre informazioni necessarie devono essere fornite al Garante solo a richiesta di questa Autorità *(clausole nn. 4, 5 e 8; art. 31, comma 2, legge n. 675/1996)*;

c) deve essere comunicata al Garante la scelta che è stata effettuata in caso di controversia non risolta in via amichevole e sottoposta all'esame di un soggetto diverso dal Garante o dall'autorità giudiziaria *(clausola 7, par. 2 e par. 1, lett. a); art. 31, comma 2, legge n. 675/1996*);

2) si riserva in ogni caso di svolgere i necessari controlli e di adottare eventuali provvedimenti anche di blocco o di divieto di trasferimento in conformità alla legge n. 675/1996 e alla normativa comunitaria *(art. 4 e considerando n. 15 della decisione*);

3) dispone la trasmissione del presente provvedimento e dell'allegata decisione della Commissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica Italiana.

Roma, 10 ottobre 2001

*Il presidente:* RODOTÀ
*Il relatore:* RODOTÀ
*Il segretario generale:* BUTTARELLI

II

*(Atti per i quali la pubblicazione non è una condizione di applicabilità)*

# COMMISSIONE

## DECISIONE DELLA COMMISSIONE
**del 15 giugno 2001**
**relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso paesi terzi a norma della direttiva 95/46/CE**

*[notificata con il numero C(2001) 1539]*

**(Testo rilevante ai fini del SEE)**

(2001/497/CE)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [1], in particolare l'articolo 26, paragrafo 4,

considerando quanto segue:

(1) A norma della direttiva 95/46/CE, gli Stati membri devono assicurarsi che un trasferimento di dati a carattere personale verso un paese terzo possa avere luogo soltanto se il paese terzo in questione garantisce un livello adeguato di protezione dei dati e se la legislazione degli Stati membri attuativa delle altre disposizioni della direttiva viene rispettata prima del trasferimento.

(2) L'articolo 26, paragrafo 2, della direttiva 95/46/CE prevede tuttavia che gli Stati membri possano autorizzare, nel rispetto di determinate garanzie, un trasferimento o una serie di trasferimenti di dati personali verso paesi terzi che non assicurino un livello adeguato di protezione dei dati. Dette garanzie possono in particolare essere fornite dalla previsione di appropriate clausole contrattuali.

(3) A norma della direttiva 95/46/CE, il livello di protezione dei dati deve essere valutato alla luce di tutte le circostanze relative all'operazione o serie di operazioni di trasferimento di dati. Il gruppo di lavoro sulla protezione degli individui per quanto riguarda il trattamento dei dati personali costituito ai sensi della direttiva [2] ha elaborato una serie di linee direttrici per l'effettuazione di questa valutazione [3].

[1] GU L 281 del 23.11.1995, pag. 31.
[2] Indirizzo Internet del gruppo di lavoro:
http://www.europa.eu. int/comm/internal_market/en/media/dataprot/wpdocs/index.htm
[3] WP 4 (5020/97): «Primi orientamenti sui trasferimenti di dati personali verso paesi terzi — possibili modalità di verifica dell'adeguatezza», documento di discussione approvato dal gruppo di lavoro il 26 giugno 1997.
WP 7 (5057/97): «Valutazione dell'autoregolamentazione dell'industria: quando reca un contributo significativo al livello di protezione dei dati in un paese terzo?», documento di lavoro: approvato dal gruppo di lavoro il 14 gennaio 1998.
WP 9 (5005/98): «Pareri preliminari sull'impiego delle clausole contrattuali nel contesto dei trasferimenti di dati personali a paesi terzi», documento di lavoro: approvato dal gruppo di lavoro il 22 aprile 1998.
WP12: «Trasferimenti di dati personali a paesi terzi: applicazione degli articoli 25 e 26 della direttiva UE per la protezione dei dati», documento di lavoro: approvato dal gruppo di lavoro il 24 luglio 1998, disponibile sul sito Internet «europa.eu.int/comm/internal_markt/en/media.dataprot/wpdocs/wp12/en» della Commissione europea.

(4) L'articolo 26, paragrafo 2, della direttiva 95/46/CE, che consente una certa flessibilità nei riguardi di organizzazioni che debbano trasferire dati personali in paesi terzi, nonché l'articolo 26, paragrafo 4, che prevede clausole contrattuali tipo, costituiscono elementi essenziali per il mantenimento del necessario flusso di dati personali fra la Comunità europea e i paesi terzi, senza creare inutili oneri per gli operatori economici. Tali disposizioni rivestono particolare importanza in quanto è probabile che la Commissione, a breve o anche a medio termine, constati l'adeguatezza del livello di protezione ai sensi dell'articolo 25, paragrafo 6, soltanto per un numero limitato di paesi.

(5) Le clausole contrattuali tipo costituiscono soltanto una delle possibilità previste dalla direttiva 95/46/CE per la liceità dei trasferimenti di dati personali in paesi terzi, oltre a quanto previsto agli articoli 25 e 26, paragrafi 1 e 2. Sarà più agevole per le organizzazioni trasferire i dati in paesi terzi incorporando tali clausole nei contratti. Le clausole contrattuali tipo riguardano soltanto la protezione dei dati. Gli esportatori e importatori dei dati sono liberi di inserire altre clausole a carattere commerciale ritenute pertinenti ai fini del contratto, ad esempio in materia di assistenza reciproca in caso di controversie con le persone interessate dai dati o con un'autorità di controllo, purché esse non siano incompatibili con le clausole tipo.

(6) La presente decisione deve applicarsi fatte salve le eventuali autorizzazioni concesse dagli Stati membri ai sensi delle disposizioni nazionali di attuazione dell'articolo 26, paragrafo 2. La presente decisione ha esclusivamente l'effetto di vietare che gli Stati membri rifiutino di riconoscere come adeguate garanzie le clausole contrattuali in essa contenute, e non produce alcun effetto su clausole contrattuali diverse.

(7) La presente decisione si limita a prevedere che le clausole di cui all'allegato possono essere utilizzate da un responsabile del trattamento con sede nella Comunità europea come garanzie sufficienti ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46/CE. Il trasferimento di dati personali in paesi terzi costituisce un'operazione di trattamento in uno Stato membro la cui legittimità è soggetta alla legislazione nazionale. Le autorità di controllo in materia di protezione dei dati degli Stati membri, nell'esercizio di funzioni e poteri loro attribuiti ai sensi dell'articolo 28 della direttiva 95/46/CE, restano competenti per determinare se l'esportatore dei dati ha rispettato la legislazione nazionale che recepisce le disposizioni della direttiva 95/46/CE, ed in particolare eventuali norme specifiche per quanto riguarda l'obbligo di fornire informazioni a norma della direttiva.

(8) L'ambito di applicazione della presente decisione non si estende al trasferimento di dati personali, operato da responsabili del trattamento aventi sede nella Comunità a destinatari aventi sede al di fuori della Comunità, che costituiscano meri incaricati di trattamenti tecnici. Detti trasferimenti non richiedono le stesse garanzie in quanto l'incaricato del trattamento agisce esclusivamente per conto del responsabile del trattamento. La Commissione intende provvedere in ordine a questo genere di trattamenti con una successiva decisione.

(9) È opportuno stabilire le informazioni minime che le parti devono specificare nel contratto relativo al trasferimento. Gli Stati membri devono mantenere il potere di specificare le informazioni che le parti sono tenute a fornire. L''applicazione della presente decisione sarà rivista alla luce dell'esperienza acquisita.

(10) La Commissione potrà inoltre considerare in futuro se altre clausole tipo presentate da organizzazioni commerciali o altre parti interessate offrano garanzie adeguate ai sensi della direttiva 95/46/CE.

(11) Le parti devono essere libere di convenire le prescrizioni alle quali deve conformarsi l'importatore dei dati ai fini dell'effettiva protezione degli stessi, ma determinati principi di protezione devono essere applicati in qualunque circostanza.

(12) I dati devono essere trattati e successivamente utilizzati o comunicati ulteriormente soltanto per scopi determinati e non devono essere trattenuti che per il tempo strettamente necessario.

(13) Ai sensi dell'articolo 12 della direttiva 95/46/CE le persone interessate dai dati devono avere accesso a tutti i dati che le riguardano e se del caso diritto di rettifica, di cancellazione o di congelamento di determinati dati.

(14) L'ulteriore trasferimento di dati personali ad altro responsabile del trattamento, avente sede in un paese terzo, deve essere consentito soltanto subordinatamente al rispetto di determinate condizioni, tendenti in particolare a garantire che le persone interessate dai dati siano adeguatamente informate ed abbiano la possibilità di formulare osservazioni e, in casi determinati, di negare il proprio consenso al trasferimento.

(15) Oltre a verificare se i trasferimenti in paesi terzi sono conformi alla legislazione nazionale, le autorità di controllo devono inoltre svolgere un ruolo fondamentale nel meccanismo contrattuale, al fine di garantire che i dati personali siano adeguatamente protetti dopo il trasferimento. In determinate fattispecie le autorità degli Stati membri devono avere la possibilità di proibire o sospendere un trasferimento o serie di trasferimenti di dati basati sulle clausole contrattuali tipo, in relazione a casi eccezionali in cui si accerti che un trasferimento su base contrattuale avrebbe la probabile conseguenza di recare sostanziale pregiudizio alle garanzie di adeguata tutela delle persone interessate dai dati.

(16) Deve potersi esigere l'esecuzione delle clausole contrattuali tipo non soltanto su istanza delle parti che stipulano il contratto, ma anche delle persone interessate dai dati, in particolare qualora le stesse subiscano pregiudizio in conseguenza di violazioni del contratto.

(17) Il contratto deve essere retto dalla legge dello Stato membro in cui ha sede l'esportatore dei dati, che abiliti il terzo beneficiario di un contratto a ottenerne l'esecuzione. Le persone interessate dai dati devono poter essere rappresentate da associazioni o altre organizzazioni se lo desiderano e se ciò è autorizzato dalla legislazione nazionale.

(18) Per ridurre le difficoltà pratiche che le persone interessate dai dati potrebbero incontrare all'atto dell'esercizio dei loro diritti in base alle clausole contrattuali tipo, l'esportatore e l'importatore dei dati devono essere tenuti responsabili separatamente e in solido per danni derivanti da qualsiasi violazione di disposizioni soggette alla clausola del terzo beneficiario.

(19) Le persone interessate dai dati hanno diritto di azione nonché diritto al risarcimento del danno a carico dell'esportatore e dell'importatore dei dati stessi, o di entrambi, per i danni derivanti da qualsiasi atto incompatibile con gli obblighi di cui alle clausole contrattuali tipo. Entrambe le parti possono essere esonerate da tale responsabilità se dimostrano di non essere responsabili del danno.

(20) La responsabilità separatamente e in solido non si estende alle disposizioni escluse dalla clausola del terzo beneficiario, e non espone necessariamente una delle parti a responsabilità per illecito trattamento ad opera dell'altra. Benché tale reciproco indennizzo fra le parti non costituisca un requisito per l'adeguatezza della tutela delle persone interessate dai dati e le parti possano quindi eliminarlo dal contratto, esso deve essere incluso nelle clausole contrattuali tipo a fini di chiarezza e per evitare che le parti siano obbligate a concordare di volta in volta le clausole in materia di indennizzo.

(21) Qualora una disputa fra le parti e le persone interessate dai dati non possa essere risolta amichevolmente e le persone interessate invochino la clausola del terzo beneficiario, le parti convengono di riconoscere alle persone interessate dai dati la possibilità di scegliere fra la mediazione, l'arbitrato e l'azione in giudizio. La misura in cui le persone interessate dai dati potranno effettivamente esercitare tale scelta dipenderà dalla disponibilità di sistemi attendibili e riconosciuti di mediazione e di arbitrato. La mediazione ad opera delle autorità di controllo degli Stati membri deve costituire un'alternativa nel caso in cui esse la forniscano.

(22) Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito in virtù dell'articolo 29 della direttiva 95/46/CE, ha emesso un parere sul livello di protezione raggiunto in base alle clausole contrattuali tipo allegate alla presente decisione che è stato preso in considerazione per la stesura della stessa ([1]).

(23) Le disposizioni di cui alla presente decisione sono conformi al parere del comitato istituito in virtù dell'articolo 31 della direttiva 95/46/CE,

([1]) Parere n. 1/2001 adottato dal gruppo di lavoro in data 26.1.2001 (DG MARKT 5102/00 WP 38), disponibile sul sito «Europa» della Commissione europea.

HA ADOTTATO LA PRESENTE DECISIONE:

*Articolo 1*

Le clausole contrattuali tipo di cui all'allegato della presente decisione costituiscono garanzie sufficienti ai fini della tutela della riservatezza, dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi a norma dell'articolo 26, paragrafo 2, della direttiva 95/46/CE.

*Articolo 2*

La presente decisione concerne esclusivamente l'adeguatezza della tutela assicurata dalle clausole contrattuali tipo per il trasferimento di dati personali di cui all'allegato. Essa si applica fatte salve le disposizioni nazionali di attuazione di altre disposizioni della direttiva 95/46/CE relative al trattamento dei dati personali negli Stati membri.

La presente decisione non si applica al trasferimento di dati personali operato da responsabili del trattamento, aventi sede nella Comunità, a destinatari aventi sede al di fuori della Comunità, che costituiscano meri incaricati di trattamenti tecnici.

*Articolo 3*

Ai fini della presente decisione:

a) si applicano le definizioni della direttiva 95/46/CE;

b) per «categorie particolari di dati» si intendono i dati di cui all'articolo 8 di detta direttiva;

c) per «autorità di controllo» si intende l'autorità di cui all'articolo 28 di detta direttiva;

d) per «esportatore di dati» si intende il responsabile del trattamento che trasferisce dati personali;

e) per «importatore di dati» si intende il responsabile del trattamento che conviene di ricevere dati personali dall'esportatore di dati, a fini di ulteriore trattamento ai sensi della presente decisione.

*Articolo 4*

1. Fatta salva la possibilità delle competenti autorità degli Stati membri di adottare provvedimenti, al fine di garantire il rispetto delle disposizioni nazionali di attuazione delle disposizioni di cui ai capi II, III, V e VI, della direttiva 95/46/CE, dette autorità possono avvalersi dei poteri loro attribuiti per proibire o sospendere flussi di dati verso paesi terzi, a fini di tutela delle persone per quanto riguarda il trattamento dei rispettivi dati personali, qualora:

a) sia accertato che la legislazione cui è sottoposto l'importatore dei dati lo obbliga a deroghe dai pertinenti principi di protezione dei dati che eccedano quelle ritenute necessarie in una società democratica ai sensi dell'articolo 13 della direttiva 95/46/CE, e che tali deroghe siano probabilmente destinate a recare sostanziale pregiudizio alle garanzie di cui alle clausole contrattuali tipo; oppure

b) un'autorità competente abbia accertato che l'importatore dei dati non ha rispettato le clausole contrattuali; oppure

c) sia sostanzialmente probabile che le clausole contrattuali tipo di cui all'allegato non siano o non saranno rispettate, e che la prosecuzione del trasferimento comporterebbe un rischio imminente di grave pregiudizio alle persone interessate dai dati.

2. Il divieto o la sospensione cessano non appena vengono meno le ragioni che li hanno imposti.

3. Quando uno Stato membro prende provvedimenti di cui ai paragrafi 1 e 2 ne informa la Commissione, che trasmette le informazioni agli altri Stati membri.

*Articolo 5*

La Commissione valuta il funzionamento della presente decisione sulla base delle informazioni disponibili tre anni dopo la notifica della stessa agli Stati membri, e riferisce in merito alle eventuali risultanze al comitato istituito ai sensi dell'articolo 31 della direttiva 95/46/CE, ivi compreso qualsiasi elemento suscettibile di interessare la valutazione di cui all'articolo 1 della presente decisione nonché qualsiasi elemento tale da indicare che la presente decisione viene applicata in maniera discriminatoria.

*Articolo 6*

La presente decisione si applica dal 3 settembre 2001.

*Articolo 7*

La presente decisione è indirizzata agli Stati membri.

Fatto a Bruxelles, il 15 giugno 2001.

*Per la Commissione*
Frederik BOLKESTEIN
*Membro della Commissione*

*ALLEGATO*

**CLAUSOLE CONTRATTUALI TIPO**

**a norma dell'articolo 26, paragrafo 2, della direttiva 95/46/CE per il trasferimento di dati personali a paesi terzi che non garantiscono un livello adeguato di protezione**

**Nome dell'organizzazione che esporta dati:** ..............................................................................................

..............................................................................................................................................

**Indirizzo:** ..............................................................................................................................

**Tel.** ........................................ **Fax** ........................................ **E-mail:** ........................................

**Altre informazioni identificative:** ..............................................................................................

(«**l'esportatore** dei dati»)

e

**Nome dell'organizzazione che importa dati:** ..............................................................................................

..............................................................................................................................................

**Indirizzo:** ..............................................................................................................................

**Tel.** ........................................ **Fax** ........................................ **E-mail:** ........................................

**Altre informazioni identificative:** ..............................................................................................

(«**l'importatore** dei dati»)

HANNO CONVENUTO le seguenti clausole contrattuali (le «**clausole**») al fine di addurre salvaguardie adeguate per quanto riguarda la protezione della riservatezza nonché delle libertà e dei diritti fondamentali degli individui per il trasferimento dall'esportatore all'importatore dei dati personali specificati nell'appendice 1.

*Clausola 1*

**Definizioni**

Ai fini delle clausole:

a) «**dati personali**», «**categorie particolari di dati**», «**trattamento**», «**responsabile del trattamento**», «**incaricato del trattamento**», «**persona interessata**» e «**autorità di controllo**» hanno la stessa accezione di cui alla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati («la direttiva»);

b) «**l'esportatore dei dati**» è il responsabile del trattamento che trasferisce i dati personali;

c) «**l'importatore dei dati**» è il responsabile del trattamento che accetta di ricevere dati personali dall'esportatore per ulteriore trattamento in conformità alle presenti clausole, e che non è soggetto ad un sistema vigente in un paese terzo per assicurare un'adeguata protezione.

*Clausola 2*

**Particolari del trasferimento**

I particolari del trasferimento, e in particolare le categorie di dati personali ed i fini a cui vengono trasferite, sono specificati nell'appendice 1 che costituisce parte integrante delle presenti clausole.

*Clausola 3*

**Clausola del terzo beneficiario**

Le persone interessate dai dati possono chiedere l'esecuzione della presente clausola nonché della clausola 4, lettere b), c) e d), della clausola 5, lettere a), b), c), ed e), della clausola 6, paragrafi 1 e 2, nonché delle clausole 7, 9 e 11, in qualità di terzi beneficiari. Le parti non si oppongono a che le persone interessate dai dati siano rappresentate da un'associazione o da altre ogranizzazioni se lo desiderano, e se ciò è autorizzato dalla legislazione nazionale.

*Clausola 4*

**Obblighi dell'esportatore dei dati**

L'esportatore dei dati s'impegna e garantisce quanto segue:

a) il trattamento dei dati personali, compreso il loro trasferimento, viene effettuato, e continua ad essere effettuato fino al momento del trasferimento stesso, in conformità a tutte le pertinenti disposizioni (e viene notificato, se del caso, alle autorità competenti) dello Stato membro in cui ha sede l'esportatore, nel pieno rispetto delle leggi vigenti in tale Stato;

b) qualora il trasferimento riguardi speciali categorie di dati, le persone interessate vengono informate che i dati che li riguardano potrebbero essere trasmessi ad un paese terzo che non fornisce una protezione adeguata, al più tardi all'atto del trasferimento;

c) mette a disposizione, a richiesta delle persone interessate, copia delle presenti clausole; e

d) risponde entro un termine ragionevole e nella misura del possibile ad eventuali richieste delle autorità di controllo per quanto riguarda il trattamento dei dati pesonali in questione da parte dell'importatore dei dati, nonché a qualsiasi richiesta delle persone interessate per quanto riguarda il trattamento dei relativi dati da parte dell'importatore degli stessi.

*Clausola 5*

**Obblighi dell'importatore dei dati**

L'importatore dei dati s'impegna e garantisce quanto segue:

a) di non aver ragione di ritenere che la legge applicabile nel suo caso gli impedisca di adempiere agli obblighi di cui al contratto. Qualora la suddetta legge venisse modificata in termini tali da essere probabilmente destinata ad esercitare un sostanziale effetto avverso alle garanzie di cui alle clausole, l'importatore dei dati notifica la variazione all'esportatore dei dati e all'autorità di controllo del paese in cui ha sede l'esportatore. In tal caso l'esportatore dei dati ha diritto di sospendere il trasferimento e/o di rescindere il contratto;

b) a trattare i dati personali conformemente ai principi obbligatori di tutela dei dati di cui all'appendice 2,

   oppure, su esplicito consenso delle parti espresso barrando le caselle che seguono e fatto salvo il rispetto dei principi obbligatori di protezione dei dati di cui all'appendice 3, a trattare i dati sotto ogni punto di vista rispettando:

   le pertinenti disposizioni di diritto nazionale per la protezione dei diritti e delle libertà fondamentali delle persone fisiche, e in particolare il diritto alla riservatezza per quanto riguarda il trattamento dei dati personali, applicabili a un responsabile del trattamento nel paese in cui ha sede l'esportatore dei dati, oppure,

   — le pertinenti disposizioni di cui a decisioni della Commissione a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE, accertanti che un paese terzo fornisce adeguata protezione soltanto in taluni settori d'attività, purché l'importatore dei dati avente sede in tale paese terzo non sia assoggettabile a dette disposizioni, nella misura in cui le disposizioni stesse siano applicabili nel settore del trasferimento;

c) a rispondere prontamente e adeguatamente a tutte le ragionevoli richieste dell'esportatore dei dati o delle persone interessate dai dati, per quanto riguarda il trattamento dei dati personali soggetti a trasferimento, a collaborare con la competente autorità di controllo nel corso di tutte le indagini e a rispettare il parere di tale autorità di controllo per quanto riguarda il trattamento dei dati trasferiti;

d) a sottoporre a controllo, su richiesta dell'esportatore dei dati, i propri servizi di trattamento. Il controllo viene effettuato dall'esportatore dei dati o da un ente ispettivo indipendente e in possesso delle necessarie qualifiche professionali, selezionato dall'esportatore dei dati e, ove necessario, di concerto con le autorità di controllo;

e) a fornire su richiesta copia delle clausole stipulate alle persone interessate dai dati, e ad indicare la sede competente per eventuali reclami.

*Clausola 6*

**Responsabilità**

1. Le parti convengono che le persone interessate dai dati che abbiano subito pregiudizio per qualsiasi violazione delle disosizioni di cui alla clausola 3 hanno diritto di essere idennizzate dalle parti per il danno sofferto. Le parti convengono che non sussista responsabilità soltanto se dimostrino che nessuna di essi si è resa responsabile di violazioni delle dette disposizioni.

2. L'esportatore e l'importatore dei dati convengono di assumersi separatamente e in solido la responsabilità dei danni causati alle persone interessate dai dati a seguito di violazioni di cui al paragrafo 1. In caso di violazione di dette disposizioni le persone interessate dai dati possono citare in giudizio sia l'esportatore sia l'importatore dei dati, sia entrambi.

3. Le parti concordano che se una di esse viene riconosciuta responsabile di una violazione commessa dall'altra di qualsiasi disposizione di cui al paragrafo 1, la seconda delle parti indennizza la prima per ogni costo, onere, danno, spesa o perdita sostenuta dalla prima, nei limiti che gli sono imputabili (*).

*Clausola 7*

**Mediazione e giurisdizione**

1. In caso di controversie che non possano essere risolte in via amichevole fra le persone interessate dai dati e una delle parti, e qualora le persone interessate dai dati invochino la disposizione relativa al terzo beneficiario di cui alla clausola 3, le parti convengono di accettare la decisione delle persone interessate dai dati di:

a) ricorrere alla mediazione ad opera di un terzo indipendente o, se del caso, dell'autorità di controllo;

b) deferire la controversia ai tribunali dello Stato membro in cui ha sede l'esportatore dei dati.

2. le parti convengono che, di comune accordo fra le persone interessate dai dati e la relativa controparte, la risoluzione di una specifica controversia possa essere deferita ad un organo arbitrale, purché tale parte abbia sede in un paese che ha ratificato la convenzione di New York sull'applicazione dei lodi arbitrali.

3. Le parti convengono che i paragrafi 1 e 2 si applicano fatti salvi i diritti soggettivi o di azione di cui le persone interessate dai dati possono avvalersi al fine del risarcimento dei danni, in forza di altre disposizioni di diritto nazionale o internazionale.

*Clausola 8*

**Collaborazione con l'autorità di controllo**

Le parti convengono di depositare copia del presente contratto presso l'autorità di controllo su richiesta di tale autorità o se tale deposito è previsto dalla legge nazionale.

*Clausola 9*

**Scadenza delle clausole**

Le parti convengono che la scadenza delle presenti clausole, in qualsiasi circostanza e per qualsiasi motivo, non esonera le parti stesse dagli obblighi e/o condizioni di cui alle clausole stesse per quanto riguarda il trattamento dei dati trasferiti.

*Clausola 10*

**Legislazione applicabile**

Alle presenti clausole si applica la legge dello Stato membro in cui ha sede l'esportatore dei dati.

.........................................................................................................................................

*Clausola 11*

**Modifica del contratto**

Le parti si impegnano a non alterare o modificare i termini qui convenuti delle presente clausole.

**Per conto dell'esportatore dei dati:**

Cognome e nome: .........................................................................................................................

Qualifica: .........................................................................................................................

Indirizzo: .........................................................................................................................

(*) Il paragrafo 3 è facoltativo.

*Appendice 1*

**alle clausole contrattuali tipo**

**La presente appendice costituisce parte integrante delle clausole contrattuali e deve essere compilata e sottoscritta dalle parti.**

(Gli Stati membri hanno facoltà di integrare o specificare ulteriormente, in conformità alle rispettive procedure nazionali, qualsiasi altra informazione che debba fare parte della presente appendice).

*Esportatore dei dati*

(specificare brevemente le attività pertinenti al trasferimento):

..............................................................................................................................

..............................................................................................................................

..............................................................................................................................

*Importatori dei dati*

(specificare brevemente le attività pertinenti al trasferimento):

..............................................................................................................................

..............................................................................................................................

..............................................................................................................................

*Persone interessate dai dati*

I dati personali trasferiti interessano le seguenti categorie di persone (specificare):

..............................................................................................................................

..............................................................................................................................

..............................................................................................................................

*Fini del trasferimento*

Il trasferimento è necessario ai fini seguenti (specificare):

..............................................................................................................................

..............................................................................................................................

..............................................................................................................................

*Categorie di dati oggetto di trasferimento*

I dati trasferiti interessano le seguenti categorie di dati (specificare):

..............................................................................................................................

..............................................................................................................................

..............................................................................................................................

*Dati delicati* (se del caso)

Il trasferimento interessa le seguenti categorie di dati a carattere delicato (specificare):

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

*Destinatari*

I dati personali trasferiti possono essere comunicati esclusivamente ai seguenti destinatari o categorie di destinatari (specificare):

..........................................................................................................................................

..........................................................................................................................................

..........................................................................................................................................

*Limite di durata*

I dati personali trasferiti possono essere conservati soltanto per (specificare): .......................................... (mesi/anni)

| L'esportatore dei dati | L'importatore dei dati |
|---|---|
| Nome: ................................................... | Nome: ................................................... |
| ..........................................................<br>(Firma del rappresentante autorizzato) | ..........................................................<br>(Firma del rappresentante autorizzato) |

*Appendice 2*

**alle clausole contrattuali tipo**

**Principi obbligatori di protezione di cui alla clausola 5, lettera b), primo capoverso**

Questi principi di tutela dei dati devono essere letti ed interpretati alla luce delle disposizioni della direttiva 95/46/CE.

Essi si applicano fatte salve le norme imperative di diritto nazionale, cui sia soggetto l'importatore dei dati, che non eccedano quanto necessario, in una società democratica, per i motivi elencati all'articolo 13, paragrafo 1, della direttiva 95/46/CE, cioè se esse costituiscono misure necessarie alla salvaguardia della sicurezza dello Stato, della difesa, della pubblica sicurezza, della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate, di un rilevante interesse economico o finanziario dello Stato o della protezione della persona interessata o dei diritti e delle libertà altrui.

1. *Limitazione del fine*: i dati devono essere elaborati e successivamente utilizzati ovvero ulteriormente comunicati esclusivamente ai fini specificati nell'appendice allegata alle presenti clausole contrattuali tipo. I dati non possono essere detenuti più a lungo di quanto necessario ai fini per cui sono stati trasferiti.

2. *Qualità e proporzionalità dei dati*: i dati devono essere corretti e, ove necessario, aggiornati. I dati devono essere adeguati, pertinenti e non esuberanti in relazione ai fini per cui vengono trasferiti e ulteriormente trattati.

3. *Trasparenza*: gli individui interessati dai dati devono essere informati sui fini del trattamento e sull'identità del responsabile dello stesso paese terzo, e su qualsiasi altro aspetto necessario per garantire la correttezza del trattamento, salvo che queste informazioni siano già state fornite dall'esportatore dei dati.

4. *Sicurezza e riservatezza*: il responsabile del trattamento è tenuto a prendere provvedimenti tecnici ed organizzativi di sicurezza appropriati ai rischi presentati dal trattamento, come accesso non autorizzato. Qualsiasi persona che agisca in virtù dell'autorità del responsabile del trattamento non deve effettuare operazioni di trattamento dei dati se non per disposizione del responsabile del trattamento stesso.

5. *Diritti di accesso, rettifica, cancellazione e congelamento dei dati*: come previsto dall'articolo 12 della direttiva 95/46/CE, le persone interessate dai dati hanno diritto di accedere a tutti i dati oggetto di trattamento che a loro si riferiscono, nonché il diritto di rettificare, cancellare o bloccare i dati il cui trattamento non sia conforme ai presenti principi, in particolare per il carattere incompleto o inesatto dei dati stessi. Le persone interessate dai dati devono inoltre avere la possibilità di opporsi al trattamento dei dati che a loro si riferiscono per validi e legittimi motivi inerenti alla loro situazione particolare.

6. *Restrizioni sui trasferimenti successivi*: ulteriori trasferimenti di dati personali dall'importatore dei dati ad altri responsabili del trattamento con sede in un paese terzo che non fornisca protezione adeguata o non sia assoggettato a una decisione della Commissione a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE (trasferimenti successivi) possono essere effettuati soltanto:

   a) se le persone interessate dai dati abbiano dato il loro esplicito consenso al successivo trasferimento in caso si tratti di speciali categorie di dati, o abbiano avuto la possibilità di negare tale consenso negli altri casi.

      Le informazioni minime che devono essere fornite alle persone interessate devono comprendere, in una lingua che gli stessi possano capire:

      — gli scopi del successivo trasferimento,

      — l'identità dell'esportatore di dati con sede nella Comunità,

      — le categorie degli ulteriori destinatari dei dati con indicazione dei paesi di destinazione, e

      — l'indicazione che, qualora le persone interessate dai dati approvino il successivo trasferimento, i dati possono essere trattati da un responsabile del trattamento con sede in un paese ove non vi è un livello adeguato di protezione della riservatezza degli individui, oppure

   b) se l'esportatore e l'importatore dei dati convengano il rispetto delle clausole contrattuali tipo con un altro responsabile del trattamento, che diviene nuova parte contraente delle clausole stesse e assume gli stessi obblighi dell'importatore dei dati.

7. *Speciali categorie di dati*: nel caso che il trattamento riguardi dati che possano rivelare l'origine razziale o etnica, ovvero le opinioni politiche, le convinzioni religiose o filosofiche, l'adesione a sindacati, dati relativi allo stato di slaute o alla vita sessuale, nonché dati relativi a reati, condanne penali o provvedimenti di sicurezza, devono essere previste ulteriori salvaguardie ai sensi della direttiva 95/46/CE, ed in particolare idonee misure di sicurezza come trasmissione cifrata o registrazione di ogni accesso ai dati.

8. *Marketing diretto*: quando i dati vengono trattati a fini di marketing diretto, devono essere previste procedure tali da consentire ai soggetti dei dati di negare in qualsiasi momento il proprio consenso all'utilizzazione a tali fini dei dati che li riguardano.

9. *Decisioni individuali automatizzate*: le persone interessate dai dati hanno il diritto di non essere assoggettati a decisioni basate unicamente sul trattamento automatizzato di dati, a meno che non vengano presi altri provvedimenti per salvaguardare i loro legittimi interessi ai sensi dell'articolo 15 della direttiva 95/46/CE. Qualora l'obiettivo del trasferimento sia una decisione automatizzata ai sensi del citato articolo 15 la persona interessata deve avere il diritto di concoscere le motivazioni su cui si basa detta decisione.

---

*Appendice 3*

**alle clausole contrattuali tipo**

**Principi obbligatori di protezione di cui alla clausola 5, lettera b), secondo capoverso**

1. *Limitazione del fine*: i dati devono essere elaborati e successivamente utilizzati ovvero ulteriormente comunicati esclusivamente ai fini specificati nell'appendice allegata alle presente clausole contrattuali tipo. I dati non possono essere detenuti più a lungo di quanto necessario ai fini per cui sono stati trasferiti.

2. *Diritti di accesso, rettifica, cancellazione e congelamento dei dati*: come previsto dall'articolo 12 della direttiva 95/46/CE, le persone interessae dai dati hanno diritto di accedere a tutti i dati oggetto di trattamento che a loro si riferiscono, nonché il diritto di rettificare, cancellare o bloccare i dati il cui trattamento non sia conforme ai presenti principi, in particolare per il carattere incompleto o inesatto dei dati stessi. Le persone interessate dai dati devono inoltre avere la possibilità di opporsi al trattamento dei dati che a loro si riferiscono per validi e legittimi motivi inerenti alla loro situazione particolare.

3. *Restrizioni sui trasferimenti successivi*: ulteriori trasferimenti di dati personali dall'importatore dei dati ad altri responsabili del trattamento con sede in un paese terzo che non fornisca protezione adeguata o non sia assoggettato a una decisione della Commissione a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE (trasferimenti successivi) possono essere effettuati soltanto:

   a) se le persone interessate dai dati abbiano dato il loro esplicito consenso al successivo trasferimento in caso si tratti di speciali categorie di dati, o abbiano avuto la possibilità di negare tale consenso negli altri casi.

   Le informazioni minime che devono essere fornite alle persone interessate devono comprendere, in una lingua che gli stessi possano capire:
   — gli scopi del successivo trasferimento,
   — l'identità dell'esportatore di dati con sede nella Comunità,
   — le categorie degli ulteriori destinatari dei dati con indicazione dei paesi di destinazione, e
   — l'indicazione che, qualora le persone interessate dai dati approvino il successivo trasferimento, i dati possono essere trattati da un responsabile del trattamento con sede in un paese ove non vi è un livello adeguato di protezione della riservatezza degli individui, oppure

   b) se l'esportatore e l'importatore dei dati convengano il rispetto delle clausoe contrattuali tipo con un altro responsabile del trattamento, che diviene nuova parte contraente delle clausole stesse e assume gli stessi obblighi dell'importatore dei dati.

---

**01A11979**

DELIBERAZIONE 10 ottobre 2001.

**Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso organizzazioni aventi sede negli Stati Uniti effettuati in base ai "Principi di approdo sicuro in materia di riservatezza" applicati in conformità alle "Domande più frequenti" (FAQ) e all'ulteriore documentazione allegata alla decisione della Commissione europea del 26 luglio 2000, n. 2000/520/CE.** (Deliberazione n. 36).

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del Prof. Stefano Rodotà, presidente, del Prof. Giuseppe Santaniello, vice-presidente, del Prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 25, paragrafi nn. 1 e 2, della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 secondo cui i dati personali possono essere trasferiti in un Paese non appartenente all'Unione europea qualora il Paese terzo garantisca un livello di protezione adeguato, secondo quanto previsto nel paragrafo 2 del medesimo articolo;

Visto il paragrafo 6 del medesimo art. 25 secondo il quale la Commissione europea può constatare che un Paese terzo garantisce un livello di protezione adeguato ai sensi del citato paragrafo 2, ai fini della tutela della vita privata o dei diritti e delle libertà fondamentali della persona;

Vista la decisione della Commissione europea del 26 luglio 2000 n. 2000/520/CE (pubblicata sulla *Gazzetta Ufficiale delle Comunità europee* L 215 del 25 agosto 2000 e L 115 del 25 aprile 2001) secondo la quale i "Principi di approdo sicuro in materia di riservatezza" allegati alla medesima decisione, applicati in conformità agli orientamenti forniti da talune "Domande più frequenti" (FAQ) parimenti allegate, garantiscono un livello adeguato di protezione dei dati personali trasferiti dalla Comunità ad organizzazioni aventi sede negli Stati Uniti sulla base della documentazione pubblicata dal Dipartimento del commercio statunitense ivi menzionata;

Considerato che gli Stati membri europei devono adottare le misure necessarie per conformarsi alla decisione della Commissione, ai sensi del paragrafo 6 del citato art. 25 della direttiva;

Visto l'art. 28 della legge 31 dicembre 1996, n. 675 secondo cui il trasferimento dei dati personali all'estero può avvenire: *a*) qualora l'ordinamento dello Stato di destinazione o di transito dei dati assicuri un livello di tutela delle persone adeguato o, se si tratta di dati sensibili o di taluni dati di carattere giudiziario, di grado pari a quello assicurato dall'ordinamento italiano; *b*) oppure, qualora ricorra uno dei casi previsti nel comma 4 del medesimo articolo; *c*) in ogni caso, qualora sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto (comma 4, lett. g));

Ritenuta la necessità di adottare una misura necessaria per l'applicazione della Decisione della Commissione in conformità al citato art. 28, nelle more del completamento del recepimento della citata direttiva n. 95/46/CE;

Ritenuto che i sette Principi allegati alla Decisione e precisati in n. 15 FAQ, su cui si è espresso con vari pareri ed osservazioni anche il Gruppo delle autorità garanti europee di cui all'art. 29 della citata direttiva, prevedono alcune garanzie per i diritti dell'interessato che in conformità al diritto comunitario vanno ritenute adeguate ai sensi del citato art. 28, comma 4, lett. g);

Considerato che i soggetti che applicano i predetti Principi possono prevedere ulteriori garanzie per le persone cui si riferiscono i dati, rispetto a quelle minime previste dalla richiamata Decisione;

Rilevato che la Decisione della Commissione può essere adattata alla luce dell'esperienza acquisita nella sua attuazione o alla luce di nuove normative intervenute negli Stati Uniti (art. 4);

Visti gli articoli 2 e 3 della Decisione in tema di controlli e provvedimenti delle autorità di garanzia degli Stati membri sulla liceità e correttezza dei trasferimenti e dei trattamenti di dati anteriori ai trasferimenti medesimi, anche in relazione a quanto previsto dall'articolo 4 della direttiva n. 95/46/CE sul diritto nazionale applicabile;

Vista la FAQ n. 5 sul ruolo che le autorità di garanzia degli Stati membri dovrebbero svolgere con la cooperazione delle organizzazioni statunitensi che ricevano dati personali dall'Unione europea, anche nell'ambito di un comitato (*panel*) informale di autorità costituito a livello europeo cui il Garante intende partecipare;

Rilevato che le autorità di garanzia degli Stati membri, riunite nel Gruppo di cui all'art. 29 della direttiva europea n. 95/46/CE, hanno aderito all'inserimento della FAQ n. 5 nel pacchetto di misure previsto dalla Decisione della Commissione;

Ritenuta la necessità di assicurare ulteriore pubblicità ai predetti Principi disponendo la loro pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana in allegato alla presente autorizzazione;

Vista la documentazione d'ufficio;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il prof. Giuseppe Santaniello;

TUTTO CIO' PREMESSO IL GARANTE:

1) autorizza i trasferimenti di dati personali dal territorio dello Stato verso organizzazioni aventi sede negli Stati Uniti effettuati sulla base e in conformità ai "Principi di approdo sicuro in materia di riservatezza", applicati in conformità alle "Domande più frequenti" (FAQ) e all'ulteriore documentazione allegata alla Decisione della Commissione europea del 26 luglio 2000 n. 2000/520/CE;

2) si riserva di svolgere, in conformità alla normativa comunitaria, alla legge n. 675/1996, all'art. 3 della Decisione della Commissione e all'allegata FAQ. n. 5, i necessari controlli sulla liceità e correttezza dei trasferimenti e delle operazioni di trattamento anteriori ai trasferimenti medesimi, nonché sul rispetto dei predetti Principi, e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento;

3) dispone la trasmissione del presente provvedimento e dell'allegata decisione della Commissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica Italiana.

Roma, 10 ottobre 2001

*Il presidente:* RODOTÀ
*Il relatore:* SANTANIELLO
*Il segretario generale:* BUTTARELLI

**DECISIONE DELLA COMMISSIONE**

**del 26 luglio 2000**

**a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti**

*[notificata con il numero C(2000) 2441]*

**(Testo rilevante ai fini del SEE)**

(2000/520/CE)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [1], in particolare l'articolo 25, paragrafo 6,

considerando quanto segue:

(1) A norma della direttiva 95/46/CE, gli Stati membri sono tenuti a consentire il trasferimento verso un paese terzo di dati personali soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato e se vengono rispettate, prima del trasferimento stesso, norme di attuazione delle altre disposizioni della direttiva adottate dagli Stati membri.

(2) La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. In tal caso è possibile trasferire dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.

(3) A norma della direttiva 95/46/CE, il livello di protezione dei dati personali deve essere valutato con riguardo a tutte le circostanze relative a un trasferimento o a una categoria di trasferimenti di dati e nel rispetto di determinate condizioni; il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali [2] ha fornito indicazioni circa le modalità di effettuazione di tali valutazioni [3].

(4) Tenuto conto della diversità degli approcci in materia di tutela dei dati nei paesi terzi, la valutazione dell'adeguatezza e le decisioni a norma dell'articolo 25, paragrafo 6, della direttiva 95/46/CE devono essere eseguite in modo da non produrre discriminazioni arbitrarie o ingiustificate nei confronti dei paesi terzi o fra questi, qualora sussistano condizioni analoghe, e da non costituire ostacoli dissimulati agli scambi, tenendo conto degli attuali impegni internazionali della Comunità.

(5) Per il trasferimento di dati dalla Comunità agli Stati Uniti, il livello adeguato di protezione di cui alla presente decisione sarebbe raggiunto ove le organizzazioni si conformino ai «principi dell'approdo sicuro in materia di riservatezza» («The Safe Harbor Privacy Principles»), in prosieguo «i principi», nonché alle «domande più frequenti» («Frequently Asked Questions»), in prosieguo «FAQ», pubblicate dal governo degli Stati Uniti in data 21 luglio 2000, che forniscono indicazioni per l'attuazione dei principi stessi. Le organizzazioni devono inoltre rendere note pubblicamente le loro politiche in materia di riservatezza e sono sottoposte all'autorità della Commissione federale per il commercio (FTC) ai sensi della sezione 5 del Federal Trade Commission Act, che vieta attività o pratiche sleali o ingannevoli in materia commerciale o collegata al commercio, oppure di altri organismi istituiti con legge in grado di assicurare efficacemente il rispetto dei principi applicati in conformità alle FAQ.

(6) I settori e/o le attività di elaborazione dei dati non sottoposti all'autorità di alcun ente governativo degli Stati Uniti di cui all'allegato VII non rientrano nell'ambito della presente decisione.

(7) Al fine di assicurare la corretta applicazione della presente decisione, è necessario che le organizzazioni che aderiscono ai principi ed alle FAQ possano essere riconosciute dalle parti interessate, quali le persone che sono oggetto dei dati, gli esportatori di dati e le autorità per la protezione dei dati; a tal fine il Dipartimento del com-

[1] GU L 281 del 23.11.1995, pag. 31.

[2] L'indirizzo web del gruppo di lavoro è il seguente: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

[3] WP 12: Trasferimenti di dati personali a paesi terzi: applicazione degli artt. 25 e 26 della direttiva UE sulla protezione dei dati, documento approvato dal gruppo di lavoro il 24 luglio 1998.

mercio degli Stati Uniti, o l'ente da esso designato, deve assumersi il compito di compilare e rendere disponibile al pubblico un elenco delle organizzazioni che autocertificano la loro adesione ai principi applicati in conformità alle FAQ e sono sottoposte all'autorità di almeno uno degli enti governativi di cui all'allegato VII della presente decisione.

(8) Nell'interesse della trasparenza, e per salvaguardare la facoltà delle competenti autorità degli Stati membri di assicurare la protezione degli individui riguardo al trattamento dei dati personali, è necessario che la presente decisione specifichi le circostanze eccezionali in cui può essere giustificata la sospensione di specifici flussi di dati anche in caso di constatazione di adeguata protezione.

(9) L'approdo sicuro creato dai principi e dalle FAQ può richiedere una revisione alla luce dell'esperienza e degli sviluppi riguardanti la tutela della vita privata in un contesto in cui la tecnologia rende sempre più facile il trasferimento e il trattamento dei dati personali, e dei risultati delle attività di applicazione e di esecuzione da parte delle autorità competenti.

(10) Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE si è espresso sul livello di protezione garantito dai principi di «approdo sicuro» negli Stati Uniti. In sede di elaborazione della presente decisione si è tenuto conto dei pareri espressi da tale gruppo ([4]).

(11) Le misure previste dalla presente decisione sono conformi al parere del comitato istituito dall'articolo 31 della direttiva 95/46/CE,

([4]) WP 15: Parere 1/99 concernente il livello di protezione dei dati negli Stati Uniti e le discussioni in corso fra la Commissione europea e gli Stati Uniti.
WP 19: Parere 2/99 sull'adeguatezza dei principi internazionali dell'approdo sicuro pubblicati dal Dipartimento del commercio degli Stati Uniti il 19 aprile 1999.
WP 21: Parere 4/99 sulle domande più frequenti (FAQ) che devono essere pubblicate dal Dipartimento del commercio degli Stati Uniti in relazione ai proposti principi dell'approdo sicuro sull'adeguatezza dei principi internazionali dell'approdo sicuro.
WP 23: Documento di lavoro sull'attuale stato delle discussioni in corso fra la Commissione europea ed il governo degli Stati Uniti concernenti i principi internazionali dell'approdo sicuro.
WP 27: Parere 7/99 sul livello della protezione dei dati fornito dai principi dell'approdo sicuro pubblicati unitamente alle domande più frequenti (FAQ) e agli altri documenti relativi il 15 e 16 novembre 1999 dal Dipartimento del commercio degli Stati Uniti.
WP 31: Parere 3/2000 sul dialogo UE/USA concernente l'accordo sull'approdo sicuro.
WP 32: Parere 4/2000 sul livello di protezione fornito dai principi dell'approdo sicuro.

HA ADOTTATO LA PRESENTE DECISIONE:

*Articolo 1*

1. Ai fini dell'applicazione dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, per tutte le attività che rientrano nel campo di applicazione di detta direttiva, si considera che i «Principi di approdo sicuro in materia di riservatezza», in prosieguo i «principi», di cui all'allegato I della presente decisione, applicati in conformità agli orientamenti forniti dalle «Domande più frequenti» (FAQ) di cui all'allegato II della presente decisione, pubblicate dal Dipartimento del commercio degli Stati Uniti in data 21 luglio 2000, garantiscano un livello adeguato di protezione dei dati personali trasferiti dalla Comunità a organizzazioni aventi sede negli Stati Uniti sulla base della seguente documentazione pubblicata dal Dipartimento del commercio degli Stati Uniti:

a) riepilogo delle modalità di esecuzione dei principi di approdo sicuro, di cui all'allegato III;

b) memorandum sui danni per violazioni della riservatezza ed autorizzazioni esplicite previste dalle leggi degli Stati Uniti, di cui all'allegato IV;

c) lettera della Commissione federale per il commercio (FTC), di cui all'allegato V;

d) lettera del Dipartimento dei trasporti degli Stati Uniti, di cui all'allegato VI.

2. Le seguenti condizioni devono sussistere in relazione a ogni singolo trasferimento di dati:

a) l'organizzazione che riceve i dati si è chiaramente e pubblicamente impegnata a conformarsi ai principi applicati in conformità alle FAQ, e

b) detta organizzazione è sottoposta all'autorità prevista per legge di un ente governativo degli Stati Uniti, compreso nell'elenco di cui all'allegato VII, competente ad esaminare denunce e a imporre la cessazione di prassi sleali e fraudolente nonché a disporre il risarcimento di qualunque soggetto, a prescindere dal paese di residenza o dalla nazionalità, danneggiato a seguito del mancato rispetto dei principi applicati in conformità alle FAQ.

3. Le condizioni di cui al paragrafo 2 sono considerate soddisfatte per ogni organizzazione che autocertifica la sua adesione ai principi applicati in conformità alle FAQ a partire dalla data di notifica al Dipartimento del commercio degli Stati Uniti (o all'ente da esso designato) del pubblico annuncio dell'impegno di cui al paragrafo 2, lettera a), e dell'identità dell'ente governativo di cui al paragrafo 2, lettera b).

*Articolo 2*

La presente decisione dispone soltanto in merito all'adeguatezza della protezione offerta negli Stati Uniti, in base ai principi applicati in conformità alle FAQ, al fine di quanto prescritto dall'articolo 25, paragrafo 1, della direttiva 95/46/CE. Essa nulla dispone relativamente all'applicazione di altre disposizioni della stessa direttiva, relative al trattamento di dati personali all'interno degli Stati membri e in particolare dell'articolo 4 della stessa.

*Articolo 3*

1. Fatto salvo il loro potere di adottare misure per garantire l'ottemperanza alle disposizioni nazionali adottate in forza di disposizioni diverse dall'articolo 25 della direttiva 95/46/CE, le autorità competenti degli Stati membri possono avvalersi dei loro poteri, al fine di tutelare gli interessati con riferimento al trattamento dei dati personali che li riguardano, per sospendere flussi di dati diretti a un'organizzazione che ha autocertificato la sua adesione ai principi applicati in conformità alle FAQ nei casi in cui:

a) gli enti governativi degli Stati Uniti di cui all'allegato VII della presente decisione, o un organismo indipendente di ricorso ai sensi della lettera a) del «principio di esecuzione» di cui all'allegato I della presente decisione abbiano accertato che l'organizzazione viola i principi applicati in conformità alle FAQ, oppure

b) sia molto probabile che i principi vengano violati; vi siano ragionevoli motivi per ritenere che l'organismo di esecuzione competente non stia adottando o non adotterà misure adeguate e tempestive per risolvere un caso concreto, la continuazione del trasferimento dei dati potrebbe determinare un rischio imminente di gravi danni per gli interessati e le autorità competenti dello Stato membro abbiano fatto il possibile, date le circostanze, per informare l'organizzazione dandole l'opportunità di replicare.

La sospensione dei flussi deve cessare non appena sia garantito il rispetto dei principi applicati in conformità alle FAQ e ciò sia stato notificato alle competenti autorità dell'UE.

2. Gli Stati membri comunicano immediatamente alla Commissione l'adozione di misure a norma del paragrafo 1.

3. Gli Stati membri e la Commissione s'informano altresì a vicenda in merito ai casi in cui l'azione degli organismi responsabili non garantisca la conformità ai principi applicati in conformità alle FAQ negli Stati Uniti.

4. Ove le informazioni di cui ai paragrafi 1, 2 e 3 del presente articolo provino che uno degli organismi incaricati di garantire la conformità ai principi applicati conformemente alle FAQ negli Stati Uniti non svolge la sua funzione in modo efficace, la Commissione ne informa il Dipartimento del commercio degli Stati Uniti e, se necessario, presenta progetti di misure secondo la procedura istituita dall'articolo 31 della direttiva 95/46/CE, al fine di annullare o sospendere la presente decisione o limitarne il campo d'applicazione.

*Articolo 4*

1. La presente decisione può essere adattata in qualsiasi momento alla luce dell'esperienza acquisita nella sua attuazione e/o qualora il livello di protezione offerta dai principi e dalle FAQ sia superato dai requisiti della legislazione degli Stati Uniti. La Commissione valuta in ogni caso l'applicazione della presente decisione tre anni dopo la sua notifica agli Stati membri sulla base delle informazioni disponibili e comunica qualsiasi riscontro al comitato istituito dall'articolo 31 della direttiva 95/46/CE, fornendo altresì ogni indicazione che possa influire sulla valutazione relativa all'adeguata salvaguardia offerta dalla disposizione di cui all'articolo 1 della presente decisione, ai sensi dell'articolo 25 della direttiva 95/46/CE, nonché di eventuali applicazioni discriminatorie della decisione stessa.

2. La Commissione, se necessario, presenta progetti di opportuni provvedimenti in conformità alla procedura di cui all'articolo 31 della direttiva 95/46/CE.

*Articolo 5*

Gli Stati membri adottano le misure necessarie per conformarsi alla presente decisione entro 90 giorni dalla data di notifica delle stesse.

*Articolo 6*

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 26 luglio 2000.

*Per la Commissione*
Frederik BOLKESTEIN
*Membro della Commissione*

*ALLEGATO I*

**PRINCIPI DI APPRODO SICURO (SAFE HARBOR)**

**del dipartimento del commercio degli Stati Uniti, 21 luglio 2000**

Il 25 ottobre 1998 è entrata in vigore la legislazione globale dell'Unione europea in tema di riservatezza dei dati personali, ossia la direttiva sulla protezione dei dati (nel seguito «la direttiva»). Tale documento dispone che i dati personali possano venir trasferiti solamente in paesi non appartenenti all'UE che garantiscano un livello «adeguato» di protezione della riservatezza. Per quanto Stati Uniti ed Unione europea condividano il principio di rafforzare la tutela della sfera privata dei rispettivi cittadini, gli Stati Uniti applicano un metodo diverso da quello adottato dall'Unione europea. Gli Stati Uniti si basano su un approccio settoriale costituito da una combinazione di legislazione, regolamentazione e autoregolamentazione. Viste le differenze, molte organizzazioni americane hanno manifestato incertezze sull'impatto dello standard UE di «adeguatezza» per quanto riguarda il trasferimento di dati personali dall'Unione europea agli Stati Uniti.

Per ridurre tale incertezza e inserire tali trasferimenti in un contesto normativo più chiaro, il Dipartimento del commercio sta provvedendo a pubblicare sotto la propria autorità statutaria questo documento e le Frequently Asked Questions («i principi») al fine di incoraggiare, promuovere e sviluppare il commercio internazionale. I principi sono stati messi a punto in consultazione con l'industria e con il grande pubblico per facilitare gli scambi commerciali fra Stati Uniti ed Unione europea. Essi sono destinati unicamente ad organizzazioni americane che ricevono dati personali dall'Unione europea, al fine di permettere a tali organizzazioni di ottemperare al principio di «approdo sicuro» ed alla presunzione di «adeguatezza» che esso comporta. Giacché questi principi sono stati concepiti esclusivamente a tal fine una loro estensione ad altri fini può non risultare opportuna. I principi non possono sostituirsi alle disposizioni nazionali che recepiscono la direttiva applicabile al trattamento dei dati personali negli Stati membri.

La decisione di un'organizzazione di qualificarsi per l'approdo sicuro è puramente volontaria, e la qualifica può essere ottenuta in vari modi. Le organizzazioni che decidono di aderire a questi principi devono rispettarli al fine di ottenere e mantenere i vantaggi risultanti dall'approdo sicuro e devono dichiarare pubblicamente il loro impegno in tal senso. Si qualifica ad esempio un'organizzazione che aderisca ad un programma di tutela della riservatezza, messo a punto dal settore privato e tale da ottemperare ai principi in questione. Per qualificarsi le organizzazioni possono anche sviluppare proprie politiche in fatto di riservatezza dei dati personali, purché queste siano conformi ai principi indicati. Se un'organizzazione aderisce a un programma di tutela della riservatezza o sviluppa politiche proprie in questo senso, il mancato rispetto dei principi da parte sua è perseguibile in forza delle disposizioni contenute nella sezione 5 del Federal Trade Commission Act, che proibisce atti sleali e ingannevoli, o di disposizioni analoghe che proibiscano tali atti. (Si veda nell'appendice l'elenco degli organi statutari degli Stati Uniti riconosciuti dall'Unione europea.) Inoltre, anche le organizzazioni soggette a disposizioni (o a norme) legislative, regolamentari, amministrative o d'altro tipo che tutelino efficacemente la riservatezza dei dati personali possono compiere quanto necessario per godere dei vantaggi dell'approdo sicuro. In ogni caso, i vantaggi dell'approdo sicuro si applicano dalla data in cui le organizzazioni che desiderano qualificarsi notificano al Dipartimento del commercio o alle istanze da esso designate la propria adesione a tali principi a norma degli orientamenti illustrati nell'allegato sull'autocertificazione intitolato Frequently Asked Questions.

L'adesione a tali principi può essere limitata: a) se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia; b) da disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione; oppure c) se la direttiva o la legislazione degli Stati membri rendono possibili eccezioni o deroghe, a condizione che tali eccezioni o deroghe si applichino in contesti comparabili. Coerentemente con l'obiettivo di una maggiore tutela della sfera privata le organizzazioni devono fare il possibile per attuare detti principi integralmente ed in modo trasparente, specificando nelle rispettive politiche in materia di tutela della sfera privata in quali casi saranno regolarmente applicate le eccezioni ammesse dal punto b). Per lo stesso motivo, quando i principi e/o la legislazione statunitense consentono tale scelta, le organizzazioni sono tenute a scegliere, per quanto possibile, la protezione più elevata.

Per ragioni pratiche o d'altro tipo le organizzazioni possono voler applicare i principi a tutte le loro attività d'elaborazione; l'obbligo di applicarli vale però soltanto per i dati trasferiti dopo la loro adesione all'approdo sicuro. Allo scopo di qualificarsi per l'approdo sicuro le organizzazioni non sono tenute ad applicare i relativi principi ad informazioni archiviate in sistemi a funzionamento manuale. Le organizzazioni che desiderino beneficiare dell'approdo sicuro per ricevere trasferimenti d'informazioni dall'UE archiviate in sistemi a funzionamento manuale devono applicare i principi

a tutte le informazioni trasferite successivamente alla loro adesione all'approdo sicuro. Le organizzazioni che desiderano estendere i benefici dell'approdo sicuro ad informazioni personali trasferite dall'UE e riguardanti le risorse umane nel contesto di un rapporto di lavoro lo devono menzionare nell'autocertificazione da trasmettere al Dipartimento del commercio o alle istanze da esso designate ed uniformarsi ai requisiti elencati nelle FAQ relative all'autocertificazione. Le organizzazioni devono essere in grado di fornire le garanzie richieste dall'articolo 26 della direttiva anche qualora, per garantire autonomamente la riservatezza dei dati, si servano dei principi in accordi scritti con terzi che trasferiscono dati dall'UE, una volta che la Commissione o gli Stati membri abbiano approvato le altre disposizioni relative a tali contratti modello.

La legislazione statunitense si applica a tutte le questioni riguardanti l'interpretazione e il rispetto dei principi dell'approdo sicuro (incluse le FAQ) nonché alle relative politiche di riservatezza delle organizzazioni che vi aderiscono, eccetto quelle che si sono impegnate a cooperare con le autorità europee di tutela dei dati. Salvo disposizioni contrarie, sono sempre applicabili i principi dell'approdo sicuro e le Frequently Asked Questions.

Per «dati personali» ed «informazioni personali» s'intendono dati e informazioni, riguardanti singoli individui (identificati od identificabili) cui si applichi la direttiva, che un'organizzazione statunitense riceve dall'Unione Europea e registra in qualsiasi forma.

## NOTIFICA

Le organizzazioni devono informare i singoli individui in merito alle finalità per cui vengono raccolte e utilizzate le informazioni su di essi, alle modalità per contattare le organizzazioni in relazione ad eventuali quesiti o reclami, alla tipologia dei terzi a cui vengono fornite le informazioni, e infine ad opzioni e mezzi che le organizzazioni mettono a disposizione dei singoli individui per limitare l'utilizzazione e la rivelazione delle informazioni. Queste indicazioni vanno formulate in un linguaggio chiaro e in modo da attirare l'attenzione quando si tratti del primo invito a fornire informazioni personali alle organizzazioni rivolto ad una persona oppure non appena ciò risulti successivamente possibile, ma comunque prima che le organizzazioni utilizzino o rivelino per la prima volta a terzi tali informazioni per finalità diverse da quelle per le quali le informazioni stesse erano state originariamente raccolte (1).

## SCELTA

Un'organizzazione deve offrire agli individui la possibilità di scegliere (facoltà di rifiuto) se le informazioni personali che li riguardano vadano a) rivelate a terzi (1), ovvero b) utilizzate per fini incompatibili con quelli per cui le informazioni stesse erano state originariamente raccolte o con quelli successivamente autorizzati dall'interessato. Agli interessati andranno forniti mezzi chiari, agevolmente riconoscibili in quanto tali, di rapida fruizione e di costo accettabile per esercitare la propria scelta.

Per le informazioni di carattere delicato (ossia informazioni personali concernenti condizioni mediche o sanitarie, origine etnica o razziale, opinioni politiche, credenze filosofiche o religiose, appartenenza a sindacati, o la vita sessuale dell'individuo), va data la possibilità di scelta affermativa o esplicita (facoltà di consenso) per quanto riguarda la possibilità che le informazioni in questione vengano rivelate a terzi od utilizzate per scopi diversi da quelli per cui esse erano state originariamente raccolte o da quelli successivamente autorizzati dagli interessati con l'esercizio della facoltà di consenso. Un'organizzazione è in ogni caso tenuta a considerare di carattere delicato qualsiasi informazione ricevuta da un terzo che la definisca e la consideri tale.

## TRASFERIMENTO SUCCESSIVO

Le organizzazioni che comunicano informazioni a terzi devono applicare i principi di notifica e di scelta. Un'organizzazione che intende trasferire informazioni a terzi che agiscono in qualità di rappresentanti, come specificato nella nota, lo può fare a condizione di accertarsi prima che questi ultimi aderiscono ai principi dell'approdo sicuro, o rientrano nel campo d'applicazione della direttiva o di un'altra forma d'accertamento dell'idoneità, ovvero di stipulare con i terzi un accordo scritto che comporti per essi l'obbligo di offrire almeno lo stesso livello di protezione della riservatezza richiesto dai relativi principi. Un'organizzazione che ottemperi a tali prescrizioni non può essere ritenuta responsabile (salvo che non abbia concordato altrimenti) se i terzi, cui ha trasferito l'informazione, la elaborano secondo modalità contrarie a quanto imposto o dichiarato, a meno che l'organizzazione stessa non fosse od avesse dovuto essere a conoscenza del fatto che i terzi in questione avrebbero proceduto in tal modo e non abbia preso provvedimenti ragionevoli per impedire che ciò accadesse o porvi termine.

---

(1) Non occorre informare l'interessato od offrirgli la possibilità di scelta quando le informazioni vengono trasmesse ad un terzo che agisce in qualità di rappresentante per eseguire uno o più compiti a nome dell'organizzazione ed obbedendo ad istruzioni da essa ricevute. A tali trasmissioni si applica per contro il principio del trasferimento successivo.

**SICUREZZA**

Le organizzazioni che detengono, aggiornano, utilizzano o diffondono informazioni personali devono prendere ragionevoli precauzioni per proteggerle da perdita ed abusi nonché da accesso, rivelazione, alterazione e distruzione non autorizzati.

**INTEGRITÀ DEI DATI**

Conformemente a questi principi le informazioni personali devono risultare pertinenti ai fini per cui sono state raccolte od a quelli successivamente autorizzati dagli interessati. Se ed in quanto necessario per tali fini un'organizzazione deve prendere provvedimenti ragionevoli per garantire che i dati siano attendibili in funzione dell'uso che si prevede di farne, accurati, completi e aggiornati.

**ACCESSO**

Gli individui devono poter accedere alle informazioni personali che li riguardano in possesso di una data organizzazione, ed altresì poterle correggere, emendare o cancellare se ed in quanto esse risultino inesatte, salvo il caso specifico in cui l'onere o la spesa che tale accesso comporta siano sproporzionati ai rischi per la riservatezza degli interessati oppure vengano violati i diritti di persone che non siano i diretti interessati.

**GARANZIE D'APPLICAZIONE**

Per tutelare efficacemente la riservatezza dei dati personali occorre disporre meccanismi volti a garantire il rispetto dei principi, la possibilità di ricorso per gli individui cui si riferiscono i dati che vedano lesi i propri interessi dal mancato rispetto dei principi stessi, e la non impunità di un'organizzazione che non rispetti i principi. Nel novero di detti meccanismi devono rientrare come minimo: a) meccanismi di ricorso indipendenti, di pronto impiego e di costo accessibile, atti a consentire d'istruire e dirimere qualsiasi ricorso o contenzioso individuale grazie all'applicazione dei principi nonché di riconoscere gli indennizzi del caso laddove questa possibilità sia contemplata dalla legge o da iniziative del settore privato; b) procedure di controllo per verificare la veridicità di attestati e affermazioni rilasciati dalle organizzazioni riguardo alle proprie pratiche in fatto di riservatezza dei dati personali e l'effettivo rispetto degli impegni presi a questo proposito; e c) l'obbligo di rimediare ad eventuali problemi insorti in seguito al mancato rispetto dei principi da parte di organizzazioni che dichiarino di aderirvi, con precisazione delle conseguenze che ciò comporta per tali organizzazioni. Le sanzioni devono risultare sufficientemente rigorose da garantire il rispetto dei principi da parte delle organizzazioni.

---

*Appendice*

**Elenco degli organi statutari degli Stati Uniti riconosciuti dall'Unione europea**

L'Unione europea riconosce i seguenti organi amministrativi degli Stati Uniti come autorizzati ad esaminare le denunce e a ottenere provvedimenti inibitori di pratiche sleali o fraudolente nonchè l'indennizzo delle persone in caso di inosservanza dei principi applicati conformemente alle FAQ:

— Federal Trade Commission, in virtù delle attribuzioni che le sono conferite dalla sezione 5 del Federal Trade Commission Act;

— Department of Transportation, in virtù delle attribuzioni che gli sono conferite dal titolo 49 del United States Code, sezione 41712.

---

*ALLEGATO II*

DOMANDE PIÙ FREQUENTI (FAQ)

**FAQ 1 — Dati sensibili**

D: *Un'organizzazione deve sempre fornire una scelta esplicita (opt-in choice) in relazione a dati sensibili?*

R: No, tale scelta non è prescritta quando l'elaborazione dei dati in questione abbia luogo: 1) nel vitale interesse del diretto interessato o di un'altra persona; 2) per fini connessi alla necessità di far valere un diritto o presentare una difesa in tribunale; 3) per necessità connesse all'assistenza sanitaria a fini diagnostici; 4) nell'ambito delle attività legittime di una fondazione, di un'associazione o di qualsiasi altra organizzazione senza fini di lucro con finalità politiche, filosofiche, religiose o sindacali, a condizione che l'attività d'elaborazione riguardi unicamente i membri di tale organizzazione o le persone che sono in regolare contatto con essa nel perseguimento delle sue finalità, e che i dati non vengano rivelati a terzi senza il consenso dei diretti interessati; 5) per adempiere agli obblighi che competono ad un'organizzazione in forza della vigente legislazione sul lavoro; ovvero 6) in riferimento a dati resi manifestamente pubblici dal diretto interessato.

**FAQ 2 — Eccezioni giornalistiche**

D: *Tenuto conto della tutela che la costituzione statunitense garantisce alla libertà di stampa nonché dell'esenzione accordata dalla direttiva al materiale giornalistico, i principi dell'«approdo sicuro» si applicano anche alle informazioni di natura personale raccolte, conservate o divulgate per scopi giornalistici?*

R: Laddove il diritto alla libertà di stampa, sancito dal primo emendamento della Costituzione statunitense, interferisca con gli interessi legati alla protezione della sfera privata l'equilibrio tra gli interessi in causa è disciplinato dal primo emendamento per quanto riguarda le attività di persone od organizzazioni statunitensi. Indipendentemente dal fatto che se ne faccia o no impiego, non sottostanno alle prescrizioni in tema di «approdo sicuro» le informazioni personali raccolte per pubblicazioni, trasmissioni radiotelevisive od altre forme di comunicazione pubblica di materiale giornalistico, e neppure quelle rinvenute in materiale già pubblicato e divulgate a partire da archivi pubblici.

**FAQ 3 — Responsabilità accessoria**

D: *A norma dei principi dell'«approdo sicuro» gli ISP (Internet Service Providers — fornitori di servizi su Internet), i vettori di telecomunicazioni od altre organizzazioni sono giuridicamente responsabili quando per conto di un'altra organizzazione essi semplicemente trasmettono, indirizzano, commutano od archiviano temporaneamente informazioni tali da violare detti principi?*

R: No. Né la direttiva né l'«approdo sicuro» creano responsabilità accessorie. Un'organizzazione non può venir ritenuta giuridicamente responsabile se ed in quanto essa agisce puramente e semplicemente da tramite per dati personali trasmessi da terzi e non determina finalità e mezzi dell'elaborazione di tali dati.

**FAQ 4 — Attività bancarie d'investimento e revisori contabili**

D: *Le attività dei revisori contabili e dei funzionari di banche d'investimento possono comportare l'elaborazione di dati personali senza il consenso o la conoscenza degli interessati. In quali circostanze i principi di informativa, scelta e accesso consentono questo tipo di elaborazione dei dati?*

R: I funzionari di una banca d'investimento od i revisori contabili possono elaborare informazioni senza che l'interessato ne sia a conoscenza solo se ed in quanto ciò sia necessario a soddisfare prescrizioni di legge o esigenze di interesse pubblico, oppure in altre circostanze in cui l'applicazione dei principi pregiudicherebbe i legittimi interessi aziendali. Fra tali interessi rientrano il monitoraggio del rispetto, da parte delle ditte, dei loro obblighi giuridici e le legittime attività contabili, nonché la riservatezza richiesta nell'eventualità di acquisizioni, fusioni, joint ventures o transazioni analoghe effettuate da funzionari di una banca d'investimento o da revisori contabili.

**FAQ 5** [1] **— Ruolo delle Autorità per la tutela dei dati (ATD)**

D: *Quali sono le modalità per assumere e garantire l'impegno di un'organizzazione a cooperare con le Autorità dell'Unione europea per la tutela dei dati?*

R: Nel contesto dell'approdo sicuro le organizzazioni statunitensi che ricevano dati personali dall'UE devono impegnarsi ad impiegare dispositivi atti a garantire che i principi dell'approdo sicuro vengano effettivamente rispettati. Più specificamente, come stabilito dal principio del controllo (enforcement) esse devono garantire che tali dispositivi contemplino: a) la possibilità di ricorso per le persone cui i dati si riferiscono, b) procedure che consentano di verificare a posteriori che le attestazioni ed affermazioni fatte circa le prassi seguite in fatto di tutela della sfera privata corrispondono a verità, e c) l'obbligo di porre rimedio ai problemi derivanti dal mancato rispetto dei principi, con le conseguenze del caso per le organizzazioni responsabili. Un'organizzazione soddisfa i punti a) e c) del principio del controllo (enforcement) se aderisce alle norme di cui alla presente domanda per la cooperazione con le Autorità per la tutela dei dati (ATD).

Per affermare il proprio impegno a cooperare con le ATD un'organizzazione dichiara, nel quadro della certificazione per l'approdo sicuro presentata al Dipartimento del commercio (si veda la domanda n. 6 sull'autocertificazione), che essa:

1. sceglie di ottemperare a quanto prescritto ai punti a) e c) del principio di garanzia dell'applicazione delle norme sull'approdo sicuro impegnandosi a cooperare con le ATD;

2. coopererà con le ATD nelle indagini relative ai reclami presentati nel quadro dell'approdo sicuro e nella risoluzione dei relativi casi; e

3. si adeguerà a qualsiasi parere fornito dalle ATD qualora queste ritengano che l'organizzazione debba attuare specifici interventi per uniformarsi ai principi dell'approdo sicuro, anche laddove tra questi rientrino provvedimenti di riparazione o risarcimento a beneficio di chi abbia subito pregiudizio da qualsiasi forma di mancato rispetto dei principi, e fornirà alle ATD conferma scritta di aver provveduto a tali interventi.

La cooperazione delle ATD assumerà la forma d'informazioni e pareri secondo le seguenti modalità:

— il parere delle ATD verrà espresso da un comitato (panel) informale di ATD costituito a livello europeo, il quale contribuirà tra l'altro a garantire un approccio armonizzato e coerente;

— il suddetto panel fornirà alle organizzazioni statunitensi interessate il proprio parere nei casi in cui non sia risultato possibile giungere ad una soluzione per i reclami presentati da singoli individui circa l'elaborazione di informazioni personali trasferite dall'UE nell'ambito dell'approdo sicuro. Tale parere mirerà a garantire che i principi dell'approdo sicuro siano correttamente applicati e provvederà altresì ad indicare i rimedi ritenuti più opportuni dalle ATD per le persone interessate;

— il panel fornirà tali pareri quando sia interpellato dalle organizzazioni interessate e/o riceva direttamente il reclamo della persona interessata nei confronti di organizzazioni che si siano impegnate a cooperare con le ATD ai fini dell'approdo sicuro, incoraggiando e se necessario aiutando le persone interessate a rivolgersi in prima istanza ai meccanismi di ricorso interni che le organizzazioni possano offrire;

— un parere verrà espresso soltanto dopo che entrambe le parti di un contenzioso abbiano avuto ragionevoli possibilità di formulare i propri commenti ed addurre qualsiasi elemento di prova esse desiderino. Il panel cercherà di esprimere il proprio parere quanto più rapidamente possibile, nei limiti di quanto consentito dall'esigenza di garantire l'equità del procedimento (due process). Di norma il panel mirerà ad esprimere il proprio parere entro un termine di 60 giorni dalla data in cui riceve il reclamo o viene interpellato, e se possibile anche più rapidamente;

— qualora lo ritenga opportuno il panel renderà pubblici i risultati del suo esame dei reclami ad esso presentati;

— il parere fornito tramite il panel non farà nascere alcuna responsabilità giuridica per il panel stesso o per le singole ATD.

[1] Perché questa FAQ possa venir inclusa nel pacchetto è necessario il consenso delle autorità competenti per la tutela dei dati (ATD), che ne hanno discusso il testo attuale in seno al gruppo di lavoro dell'articolo 29. Una maggioranza di esse lo trova accettabile, ma le ATD sono disposte ad esprimersi in via definitiva unicamente nel contesto del parere globale fornito dal gruppo di lavoro in merito al pacchetto finale.

Come si è già rilevato, le organizzazioni che scelgono di avvalersi di quest'opzione per la soluzione dei contenziosi devono impegnarsi ad uniformarsi al parere delle ATD. Qualora un'organizzazione non si adegui ad un parere entro 25 giorni dalla data in cui viene espresso, senza fornire soddisfacenti giustificazioni di tale ritardo, il panel notifica la sua intenzione di presentare il caso alla Commissione federale del commercio o ad altri organismi statunitensi, federali o statali, giuridicamente competenti per intervenire allo scopo di garantire il rispetto della legge in casi di affermazione falsa od ingannevole, ovvero in alternativa di concludere che si è avuta una grave violazione dell'accordo di cooperazione il quale è quindi da considerarsi annullato a tutti gli effetti. In quest'ultimo caso il panel informerà il Dipartimento del commercio (o l'organismo da esso designato) affinché l'elenco dei partecipanti all'approdo sicuro possa venir modificato di conseguenza. Qualsiasi mancanza all'impegno a cooperare con il comitato ovvero al rispetto dei principi dell'approdo sicuro sarà perseguibile in quanto pratica ingannevole a norma della sezione 5 della legge relativa alla Commissione federale del commercio (FTC Act) o di altre analoghe disposizioni di legge.

Alle organizzazioni che scelgano di avvalersi di questa possibilità verrà richiesto di pagare una quota annua calcolata per coprire i costi d'esercizio del panel, e potrà inoltre venir loro richiesto di sostenere le spese di traduzione eventualmente rivelatesi necessarie per l'esame dei ricorsi o delle istanze presentate. La quota annua non supererà comunque l'importo di 500 USD, e sarà inferiore a tale importo per le imprese minori.

La possibilità di cooperare con le ATD sarà aperta alle organizzazioni aderenti all'approdo sicuro per un triennio. Qualora il numero d'organizzazioni statunitensi che scelgano di avvalersi di questa possibilità si dimostri eccessivo, le ATD provvederanno a riesaminare questa opzione prima della fine di detto periodo.

**FAQ 6 — Autocertificazione**

D: *Come può un'organizzazione autocertificare la propria adesione ai principi dell'approdo sicuro?*

R: Un'organizzazione usufruisce dei vantaggi dell'approdo sicuro dalla data in cui autocertifica al Dipartimento del commercio o ad una persona (fisica o giuridica) da esso designata l'adesione ai relativi principi, seguendo le indicazioni sotto riportate.

Per autocertificare l'adesione all'approdo sicuro un'organizzazione può fornire al Dipartimento del commercio o ad una persona (fisica o giuridica) da esso designata una lettera, firmata da un proprio funzionario in nome dell'organizzazione che intende aderire all'approdo sicuro, contenente almeno le seguenti informazioni:

1. denominazione dell'organizzazione, indirizzo postale, indirizzo di posta elettronica, numero di telefono e fax;

2. descrizione delle attività dell'organizzazione in rapporto alle informazioni personali pervenute dall'UE;

3. descrizione della politica perseguita dall'organizzazione in merito a dette informazioni personali, che precisi tra l'altro: a) dove il pubblico può prenderne conoscenza; b) la data della loro effettiva applicazione; c) l'ufficio cui rivolgersi per eventuali reclami, richieste di accesso e qualsiasi altra questione riguardante l'approdo sicuro; d) lo specifico organo statutario competente ad esaminare i ricorsi contro l'organizzazione relativi a possibili pratiche sleali od ingannevoli e a violazioni delle norme legislative e regolamentari che disciplinano la tutela della sfera privata (ed elencati nell'allegato ai principi); e) il nome dei programmi concernenti la tutela della sfera privata cui partecipa l'organizzazione; f) il metodo di verifica (per esempio all'interno della società, effettuata da terzi) ([2]), e g) il meccanismo di ricorso indipendente disponibile per indagare sui reclami non risolti.

Le organizzazioni che intendono estendere i benefici dell'approdo sicuro alle informazioni riguardanti le risorse umane trasferite dall'UE per usi nel contesto di un rapporto di lavoro possono farlo qualora esista un organo statutario competente ad esaminare i ricorsi contro l'organizzazione relativi ad informazioni riguardanti le risorse umane, elencato nell'allegato «Principi di approdo sicuro». Inoltre, devono dichiarare tale intenzione nell'autocertificazione, devono altresì dichiarare di impegnarsi a cooperare con le autorità dell'UE conformemente alle FAQ 9 e 5 come applicabili e di uniformarsi a quanto raccomandato da tali autorità.

Il Dipartimento (o la persona da esso designata) conserverà un elenco di tutte le organizzazioni che inviano queste lettere, assicurando così la disponibilità dei vantaggi legati all'approdo sicuro, ed aggiornerà tale elenco in base alle lettere annuali ed alle notifiche ricevute secondo le modalità precisate nella FAQ 11. Le lettere in questione andranno inviate con cadenza almeno annuale; l'organizzazione che non provveda a farlo verrà espunta dall'elenco

([2]) Vedere la FAQ 7 sulla verifica.

e non godrà più dei vantaggi derivanti dall'approdo sicuro. L'elenco e le lettere d'autocertificazione presentate dalle organizzazioni saranno resi pubblici. Tutte le organizzazioni che si autocertifichino per l'approdo sicuro devono segnalare nelle loro pertinenti dichiarazioni pubbliche sulla politica perseguita in tema di tutela della sfera privata che esse aderiscono ai principi dell'approdo sicuro.

L'impegno a rispettare i principi dell'approdo sicuro non viene meno col tempo per quanto riguarda i dati ricevuti nel corso del periodo durante il quale un'organizzazione gode dei vantaggi dell'approdo sicuro. Il fatto di assumerlo comporta per l'organizzazione l'obbligo di applicare i relativi principi ai dati in questione sino a quando essa continuerà a detenerli, utilizzarli o rivelarli, anche se successivamente dovesse per qualsiasi motivo abbandonare l'approdo sicuro.

Le organizzazioni che cesseranno di esistere come entità giuridica separata in seguito a fusioni o acquisizioni devono notificarlo al Dipartimento del commercio (o a chi da esso designato) anticipatamente. Nella notifica si dovrà indicare anche se l'entità acquirente o quella risultante dalla fusione 1) continuerà ad essere vincolata ai principi dell'approdo sicuro nell'applicazione della legge relativa alle fusioni o alle acquisizioni oppure 2) deciderà di autocertificare la propria adesione ai principi dell'approdo sicuro o di istituire altri meccanismi di salvaguardia, quali accordi scritti, che garantiscano l'adesione ai principi dell'approdo sicuro. Qualora non si verifichi né 1) né 2), tutti i dati acquisiti nell'ambito dell'approdo sicuro devono essere immediatamente cancellati.

Un'organizzazione non è tenuta ad applicare i principi dell'approdo sicuro a tutte le informazioni di natura personale, ma deve applicarli a tutti i dati personali che abbia ricevuto dall'UE dopo aver aderito all'approdo sicuro.

Qualsiasi dichiarazione ingannevole resa da un'organizzazione al pubblico in merito alla propria adesione ai principi dell'approdo sicuro è perseguibile dalla Commissione federale per il commercio o da un altro organo governativo competente. Le dichiarazioni ingannevoli rese al Dipartimento del commercio (od alla persona fisica o giuridica da esso designata) sono perseguibili in forza della legge sulle false dichiarazioni (False Statements Act, 18 USC § 1001).

**FAQ 7 — Verifica**

D: *Quali procedure consentono alle organizzazioni di garantire la possibilità di verificare a posteriori che le attestazioni e le affermazioni da esse fatte circa le loro pratiche in fatto di rispetto della sfera privata nell'ambito dell'approdo sicuro corrispondono a verità e che tali pratiche vengono applicate secondo le modalità descritte e conformemente ai principi dell'approdo sicuro?*

R: Per soddisfare i requisiti del principio di garanzia di applicazione un'organizzazione può comprovare la veridicità di tali attestazioni ed affermazioni mediante una valutazione autonoma o facendo ricorso a revisioni esterne.

Nell'ambito dell'impostazione basata sulla valutazione autonoma, la verifica in questione dovrebbe dimostrare che la politica che un'organizzazione dichiara pubblicamente di perseguire in materia di tutela delle informazioni personali ricevuti dall'UE è accurata, esauriente, messa in chiara evidenza, pienamente attuata ed accessibile. Dovrebbe parimenti dimostrare che la politica suddetta si uniforma ai principi dell'approdo sicuro; che le persone sono informate in merito ad eventuali procedimenti interni per dar seguito ai reclami oltre che ai dispositivi indipendenti attraverso cui possono sporgere un reclamo; che ha stabilito procedure per formare i dipendenti ad applicare tale politica, oltre che per sanzionarli se non la seguono, ed infine che ha stabilito procedure per svolgere periodicamente indagini obiettive sul rispetto dei principi adottati. Almeno una volta all'anno un funzionario od un altro rappresentante dell'organizzazione dovrebbe firmare una dichiarazione che comprovi la valutazione autonoma, ed a richiesta tale dichiarazione andrebbe posta a disposizione dei singoli individui od esibita nell'ambito di un'indagine o di un reclamo per mancato rispetto dei principi dichiarati.

Le organizzazioni dovrebbero conservare i dati riguardanti l'attuazione delle politiche da esse perseguite in fatto di rispetto della sfera privata nell'ambito dell'approdo sicuro, e porle a disposizione dell'organismo indipendente incaricato di esaminare i reclami ovvero dell'ente che ha giurisdizione sulle pratiche scorrette ed ingannevoli nel quadro d'eventuali indagini o reclami per mancato rispetto dei principi dichiarati.

Nel caso in cui l'organizzazione interessata abbia scelto di avvalersi di una revisione esterna, detta revisione deve dimostrare che la politica dell'organizzazione in fatto di dati personali ricevuti dall'UE si uniforma ai principi dell'approdo sicuro, che viene regolarmente praticata e che le persone sono informate in merito ai dispositivi indipendenti di cui dispone chi intenda sporgere un reclamo. Tra i metodi impiegati per la revisione possono rientrare senza limiti di sorta l'auditing, indagini randomizzate, l'uso di «clienti civetta» o d'idonee tecnologie. Almeno una volta all'anno l'incaricato della revisione oppure un funzionario od un altro rappresentante dell'organizzazione

dovrebbe firmare una dichiarazione che comprovi il superamento di una revisione esterna sul rispetto delle regole; a richiesta tale dichiarazione andrebbe posta a disposizione dei singoli individui od esibita nel quadro d'eventuali indagini o reclami per mancato rispetto dei principi dichiarati.

**FAQ 8 — Accesso**

***Principio dell'Accesso***

L'interessato deve avere accesso ai dati a carattere personale che lo riguardano in possesso di un'organizzazione ed essere in grado di correggerli, modificarli o cancellarli se inesatti, eccettuati i casi in cui l'onere o il costo da sostenere per permettere l'accesso siano sproporzionati rispetto ai rischi per la riservatezza dell'interessato, oppure possano essere violati diritti legittimi di terzi.

D 1: *Il diritto all'accesso è assoluto?*

R 1: No. Conformemente ai principi dell'approdo sicuro il diritto all'accesso è fondamentale per la tutela della riservatezza: in particolare, esso consente all'interessato di verificare l'esattezza dei dati che lo riguardono. L'obbligo per l'organizzazione di fornire l'accesso ai dati personali in suo possesso riguardanti un determinato individuo è tuttavia soggetto al principio della proporzionalità o ragionevolezza e, in talune situazioni, va quindi attenuato. Effettivamente il Memorandum sulle Linee guida dell'OCSE del 1980 sulla tutela della sfera privata afferma chiaramente che per un'organizzazione l'obbligo di fornire l'accesso non è assoluto. Esso non impone una ricerca scrupolosa quale quella necessaria, ad esempio, per un mandato di comparizione, né l'accesso a tutte le varie forme in cui l'organizzazione può detenere dati.

L'esperienza ha dimostrato piuttosto che, nel soddisfare le domande d'accesso degli interessati, le organizzazioni dovrebbero tener presente innanzitutto il motivo che ha indotto originariamente alla richiesta. Ad esempio, se una richiesta d'accesso è vaga o se abbraccia un settore molto ampio, l'organizzazione può avviare un dialogo con l'interessato in modo da capire meglio la motivazione della richiesta e individuare i dati per fornire la risposta. L'organizzazione potrebbe cercare di focalizzare le ricerche sulle parti dell'organizzazione con le quali la persona in questione ha interagito e/o il tipo di dati (o il loro uso) oggetto della richiesta d'accesso. I singoli interessati non sono tuttavia tenuti a motivare le richieste d'accesso ai dati che li riguardano.

Le spese e gli oneri sono fattori importanti e dovrebbero essere presi in considerazione, ma non sono determinanti nel decidere se la fornitura dell'accesso sia o no ragionevole. Se ad esempio i dati vengono utilizzati per decisioni che producono effetti rilevanti per l'interessato (come il rifiuto o la concessione di benefici importanti quali un'assicurazione, un prestito ipotecario o un lavoro), conformemente a quanto enunciato nelle altre FAQ, l'organizzazione dovrà fornirli, anche se ciò è relativamente difficile o costoso.

Se i dati richiesti non sono sensibili o non servono per decisioni con conseguenze di rilievo per l'interessato (ad esempio, dati di marketing non sensibili che servano a stabilire se inviare o no un catalogo), e sono prontamente disponibili e comunicabili a costi non eccessivi, l'organizzazione dovrebbe permettere l'accesso ai dati di fatto in suo possesso riguardanti la persona in questione. Tali dati potrebbero comprendere informazioni fornite dall'interessato ed elementi rilevati nell'ambito di una transazione o forniti da terzi ma riguardanti la persona stessa.

In omaggio alla natura fondamentale dell'accesso, le organizzazioni dovrebbero sempre impegnarsi sinceramente per consentirlo. Quando ad esempio occorra tutelare determinate informazioni che possano venir agevolmente separate da altri dati oggetto di una richiesta di accesso, l'organizzazione dovrebbe fornire le informazioni di natura non riservata espungendone quelle soggette a tutela. Se in determinate circostanze un'organizzazione ritiene di dover negare l'accesso essa dovrà motivare tale decisione e indicare al richiedente con chi prendere contatto per ottenere ulteriori delucidazioni.

D 2: *Cosa s'intende per «informazioni commerciali riservate»? Possono le organizzazioni negare l'accesso per tutelare tali informazioni?*

R 2: Le informazioni commerciali riservate (tale formulazione è utilizzata nelle norme federali di procedura civile riguardanti le invenzioni) sono informazioni che l'organizzazione ha deciso di proteggere dalla divulgazione, laddove un concorrente possa trarre un vantaggio di mercato da tale divulgazione. Possono ad esempio costituire informazioni commerciali riservate il particolare software utilizzato da un'organizzazione, un programma di

modellizzazione od alcuni suoi dettagli. Quando sia possibile separare agevolmente informazioni commerciali di natura riservata da altri dati oggetto di una richiesta d'accesso, l'organizzazione dovrebbe fornire le informazioni di natura non riservata espungendone quelle commerciali riservate. Le organizzazioni possono negare o restringere l'accesso se ed in quanto il fatto di accordarlo porterebbe a rivelare informazioni commerciali riservate che le riguardino e rispondano alla definizione datane sopra, quali profili di marketing o classificazioni elaborate dall'organizzazione, ovvero informazioni di natura commerciale riservate concernenti terzi per le quali valgano obblighi contrattuali di riservatezza, in circostanze in cui sia normale che detti obblighi di riservatezza vengano assunti od imposti.

D 3: *Nel consentire l'accesso l'organizzazione può comunicare ai richiedenti i dati personali che li riguardano estratti dalla sua base dati o deve fornire l'accesso alla base stessa?*

R 3: L'accesso può assumere la forma della comunicazione dei dati al richiedente; l'organizzazione non è tenuta a fornire l'accesso alla propria base dati.

D 4: *L'organizzazione è tenuta a ristrutturare le sue banche dati per poter fornire l'accesso?*

R 4: L'accesso va accordato solo se ed in quanto l'organizzazione detiene i dati. Il principio dell'accesso non determina di per sé stesso l'obbligo di detenere, aggiornare, riorganizzare o ristrutturare le raccolte di dati a carattere personale.

D 5: *Dalle risposte fornite si evince che in alcune circostanze l'accesso può essere negato. In quali altre circostanze le organizzazioni possono negare ai richiedenti l'accesso ai dati personali che li riguardano?*

R 5: Tali circostanze sono limitate e qualsiasi motivo che porti a rifiutare l'accesso dev'essere chiaramente determinato. Le organizzazioni possono negare l'accesso ai dati nella misura in cui la divulgazione potrebbe interferire con la tutela d'interessi pubblici importanti, quali la sicurezza nazionale, la difesa o la sicurezza pubblica. Inoltre, se i dati personali sono trattati esclusivamente a scopo di ricerca o per finalità statistiche, l'accesso può essere negato. Altri motivi di rifiuto o limitazione dell'accesso sono:

a) interferenza con l'esecuzione o l'applicazione della legge, compresi gli aspetti relativi a prevenzione, investigazione o scoperta di reati ovvero al diritto ad un giusto processo;

b) interferenza con azioni legali private, compresi gli aspetti relativi a prevenzione, investigazione o rilevazione di reclami ovvero al diritto ad un giusto processo;

c) divulgazione di dati personali riguardanti terzi, qualora tali riferimenti non possano essere soppressi;

d) violazione di un privilegio o di un obbligo legale o d'altro tipo legato alla professione;

e) mancato rispetto della necessaria riservatezza per trattative future o in corso, come quelle relative all'acquisizione d'imprese quotate in borsa;

f) pregiudizio per i controlli di sicurezza sui dipendenti o per i procedimenti per reclami;

g) pregiudizio per la riservatezza che può rivelarsi necessaria per un lasso di tempo limitato in relazione alla programmazione dell'avvicendamento del personale e alla riorganizzazione dell'impresa; ovvero

h) pregiudizio per la riservatezza che può risultare necessaria per il monitoraggio, l'ispezione o funzioni di regolamentazione connesse ad una sana gestione economica o finanziaria; ovvero

i) altre circostanze in cui l'onere o il costo da sostenere per consentire l'accesso sarebbero sproporzionati o in cui sarebbero violati diritti od interessi legittimi di terzi.

Un'organizzazione che invochi un'eccezione ha l'onere di provarla (come accade normalmente). Come già detto al richiedente andranno comunicati i motivi di rifiuto o limitazione dell'accesso ed un referente cui rivolgersi per ulteriori informazioni.

D 6: *Un'organizzazione può chiedere un contributo spese per coprire i costi derivanti dal fatto di accordare l'accesso?*

R 6: Sì. Le Linee guida dell'OCSE ammettono che le organizzazioni possano chiedere un contributo spese, a patto che non sia eccessivo. Le organizzazioni possono quindi chiedere un contributo ragionevole per l'accesso, il che permette di scoraggiare le richieste ripetitive e vessatorie.

Nel rispondere alle richieste d'accesso le organizzazioni che trattano la vendita di dati disponibili al pubblico possono pertanto farsi riconoscere i compensi abitualmente richiesti. In alternativa gli interessati possono cercare di ottenere accesso ai dati che li riguardano rivolgendosi alle organizzazioni che hanno originariamente elaborato i dati.

L'accesso non può essere rifiutato per ragioni di costo se gli interessati s'impegnano a sostenere le spese.

D 7: *Le organizzazioni sono tenute a fornire l'accesso a dati personali ricavati da basi pubbliche?*

R 7: Per chiarezza va precisato innanzitutto che le basi pubbliche sono quelle delle amministrazioni od enti pubblici di qualsiasi livello, che possono essere consultate da chiunque lo desideri. Finché tali dati non sono associati ad altri dati personali non è necessario applicare il principio dell'accesso, eccettuato il caso in cui pochi dati non provenienti da basi pubbliche siano utilizzati per indicizzare o organizzare dati di basi pubbliche. Le condizioni per la consultazione stabilite dalla giurisdizione competente devono tuttavia essere rispettate. Quando peraltro informazioni provenienti da basi pubbliche siano combinate con altri dati provenienti da basi non pubbliche (salvo che nel caso specifico visto in precedenza) le organizzazioni sono tenute a fornire l'accesso a tutti i dati, partendo dal presupposto che essi non siano soggetti ad altre eccezioni consentite.

D 8: *Il principio dell'accesso va applicato ai dati personali disponibili al pubblico?*

R 8: Come nel caso dei dati ricavati da basi pubbliche (cfr. la domanda 7) non è necessario fornire accesso ai dati di cui il pubblico possa già correttamente disporre, purché questi non siano abbinati a dati non disponibili al pubblico ([3]).

D 9: *Come possono le organizzazioni tutelarsi contro richieste di accesso ripetute o vessatorie?*

R 9: Le organizzazioni non sono tenute a rispondere a tali richieste. Per questo motivo si è stabilito che le organizzazioni possano chiedere un contributo spese ragionevole e fissare limiti ragionevoli al numero di volte in cui può essere rinnovata la richiesta d'accesso di un interessato entro un determinato lasso di tempo. Nel fissare questi limiti l'organizzazione dovrebbe prendere in considerazione fattori quali la frequenza d'aggiornamento dei dati, le finalità del loro impiego e la loro natura.

D 10: *Come possono le organizzazioni tutelarsi contro richieste di accesso illecite?*

R 10: Le organizzazioni non sono tenute ad accordare l'accesso se la richiesta non è corredata da informazioni sufficienti a confermare l'identità del richiedente.

D 11: *Vi sono limiti di tempo entro i quali le organizzazioni sono tenute a rispondere alle richieste di accesso?*

R 11: Sì, le organizzazioni dovrebbero rispondere senza eccessivi ritardi ed entro un limite di tempo ragionevole. Tale obbligo può essere soddisfatto in vari modi, come indicato nel Memorandum degli orientamenti OCSE del 1980 sulla tutela della sfera privata. Ad esempio il detentore di dati che fornisca con cadenza regolare informazioni ai diretti interessati può essere esonerato dall'obbligo di rispondere immediatamente a singole richieste.

**FAQ 9 — Risorse umane**

D 1: *Il trasferimento dall'UE agli Stati Uniti di informazioni personali raccolte nell'ambito di rapporti di lavoro è coperto dall'approdo sicuro?*

R 1: Sì; se un'impresa dell'UE trasferisce dati sui propri dipendenti (presenti o passati) a un fornitore di servizi statunitense (società capogruppo, consociata o non consociata) che aderisca all'approdo sicuro, questo trasferimento è tutelato dalle relative norme. In tali casi alla rilevazione dei dati e al trattamento da essi subito prima del trasferi-

([3]) In questo punto la Commissione aveva proposto d'inserire la frase «e fintantoché siano rispettate le condizioni eventualmente stabilite dalla competente giurisdizione».

mento si applicheranno le leggi nazionali del paese dell'UE in cui sono state raccolte le informazioni, e andranno rispettate le condizioni o restrizioni applicabili al loro trasferimento in forza di dette leggi.

I principi dell'approdo sicuro trovano applicazione esclusivamente laddove si tratti di trasferire dati identificati individualmente o d'accedervi. Le relazioni statistiche basate su dati aggregati sull'occupazione e/o l'impiego di dati resi anonimi o presentati con l'uso di pseudonimi non pongono problemi sotto il profilo della tutela della sfera privata.

D 2: *Come si applicano a tali informazioni i principi della informativa e della scelta?*

R 2: Un'organizzazione statunitense che abbia ricevuto dall'UE dati sui dipendenti nell'ambito dell'approdo sicuro può rivelarli a terzi e/o farne uso per finalità differenti unicamente se e in quanto ottempera ai principi di informativa e di scelta. Qualora ad esempio un'organizzazione intenda utilizzare a fini non occupazionali (comunicazioni commerciali, ecc.) informazioni personali rilevate nell'ambito di un rapporto di lavoro, l'organizzazione statunitense deve dare agli interessati la possibilità di scelta, a meno che essi non abbiano già autorizzato l'impiego delle informazioni in questione per tali scopi. Le scelte fatte a questo proposito non vanno inoltre strumentalizzate per limitare le opportunità occupazionali o adottare provvedimenti punitivi nei confronti dei dipendenti.

Va osservato che determinate condizioni generalmente applicabili ai trasferimenti da alcuni Stati membri possono vietare altri impieghi delle informazioni in questione, anche dopo il loro trasferimento al di fuori dell'UE, e andranno rispettate.

I datori di lavoro dovrebbero inoltre fare il possibile nei limiti del ragionevole per rispettare le preferenze dei dipendenti in fatto di tutela della sfera privata. Nel novero dei provvedimenti presi a tal fine potrebbero ad esempio rientrare quelli volti a limitare l'accesso ai dati, a rendere anonimi taluni dati o ad attribuire codici o pseudonimi se i nominativi esatti non sono richiesti per la finalità gestionale in questione.

In quanto e fino a che ciò risulti necessario a evitare ogni pregiudizio per gli interessi legittimi dell'organizzazione di procedere a promozioni e nomine o prendere decisioni analoghe relative al personale, l'organizzazione non è tenuta a ottemperare ai principi di informativa e di scelta.

D 3: *Come si applica il principio dell'accesso?*

R 3: Le FAQ sull'accesso forniscono indicazioni sui motivi che possono giustificare il rifiuto o la restrizione dell'accesso a richiesta in tema di risorse umane. Nell'Unione europea i datori di lavoro devono ovviamente rispettare la regolamentazione locale e garantire ai dipendenti comunitari l'accesso a tali informazioni secondo le modalità prescritte dalla legislazione dei rispettivi paesi, a prescindere dal luogo di trattamento e memorizzazione dei dati. L'approdo sicuro impone alle organizzazioni che elaborano tali dati negli Stati Uniti di cooperare, fornendo l'accesso direttamente o tramite il datore di lavoro dell'UE.

D 4: *Come verrà impostato il problema di garantire l'applicazione dei principi dell'approdo sicuro per i dati sui dipendenti?*

R 4: Se e in quanto le informazioni sono utilizzate soltanto nel contesto del rapporto di lavoro, la responsabilità primaria nei confronti dei dipendenti rimane del datore di lavoro nell'UE. Ne consegue che i dipendenti europei che denuncino violazioni dei loro diritti alla riservatezza e siano insoddisfatti dei risultati delle procedure interne di controllo, di reclamo e di ricorso (o di qualsiasi procedura di composizione delle controversie nell'ambito di un contratto collettivo di lavoro) dovranno rivolgersi all'autorità statale o nazionale di tutela dei dati o dei diritti dei lavoratori competente per la giurisdizione in cui lavorano. Ciò vale anche nel caso in cui le presunte irregolarità abbiano avuto luogo negli Stati Uniti, siano imputabili all'organizzazione statunitense che ha ricevuto i dati anziché al datore di lavoro, e la presunta violazione riguardi i principi dell'approdo sicuro piuttosto che le disposizioni legislative nazionali con cui è stata recepita la direttiva. Questo costituisce il sistema più efficace per orientarsi tra i vari diritti e obblighi, che spesso si accavallano, derivanti dal diritto del lavoro e dai contratti di lavoro locali e dalle diverse normative sulla tutela dei dati.

Un'organizzazione statunitense che abbia aderito all'approdo sicuro e utilizzi dati di provenienza comunitaria sulle risorse umane nel contesto di un rapporto di lavoro, e che desideri che tali trasferimenti siano coperti dall'accordo sull'approdo sicuro, deve pertanto impegnarsi a collaborare alle indagini e ad attenersi al parere delle competenti autorità dell'UE per tali casi. Le autorità per la tutela dei dati che abbiano accettato di collaborare in tal senso ne

danno informativa alla Commissione europea e al Dipartimento del commercio. Qualora un'organizzazione statunitense partecipante all'approdo sicuro desideri trasferire dati sulle risorse umane da uno Stato membro la cui autorità per la tutela dei dati non abbia dato il suo accordo, si applicano le norme di cui alla FAQ 5.

**FAQ 10 — Articolo 17: contratti**

D: *Quando si trasferiscano dati dall'UE agli USA unicamente per elaborarli è necessario stipulare un contratto, a prescindere dalla partecipazione all'«approdo sicuro» del responsabile dell'elaborazione?*

R: Sì. In Europa i titolari dei trattamenti di dati personali sono sempre tenuti a concludere un contratto quando il trasferimento ha luogo unicamente a scopo di elaborazione, indipendentemente dal fatto che questa sia effettuata all'interno o all'esterno dell'UE. Il contratto serve a proteggere gli interessi del titolare, vale a dire la persona o l'ente che stabilisce le finalità e gli strumenti del trattamento, cui incombe l'intera responsabilità dei dati nei confronti degli interessati. Nel contratto vanno specificati il tipo di elaborazione cui s'intende procedere e gli eventuali provvedimenti necessari a garantire che i dati siano conservati in modo sicuro.

Un'organizzazione statunitense che partecipi all'«approdo sicuro» e riceva informazioni personali dall'UE esclusivamente a scopo di elaborazione non è dunque tenuta ad applicare i principi a tali informazioni, in quanto il titolare del trattamento nell'UE resta responsabile nei confronti degli interessati, conformemente alle prescrizioni dell'UE applicabili (che possono essere più severe degli equivalenti principi dell'«approdo sicuro»).

Poiché all'interno dell'«approdo sicuro» è fornita una protezione adeguata, per i contratti con partecipanti all'«approdo sicuro» a scopo puramente di elaborazione non sono necessarie autorizzazioni preliminari (o tali autorizzazioni sono concesse automaticamente dagli Stati membri) com'è invece il caso per i contratti stipulati con parti che non partecipano all'«approdo sicuro» o che in ogni caso non garantiscono una protezione adeguata.

**FAQ 11 — Risoluzione delle controversie e modalità di controllo dell'applicazione (enforcement)**

D: *Come si applicano le norme derivanti dal principio della garanzia di applicazione (enforcement) per la risoluzione delle controversie, e come si procede se un'organizzazione continua a non rispettare i principi?*

R: Il principio della garanzia di applicazione (enforcement) stabilisce le norme per l'applicazione dell'approdo sicuro. Le modalità di applicazione delle norme di cui al punto b) di tale principio sono illustrate nella domanda sulla verifica (FAQ 7). La presente domanda interessa i punti a) e c), che prescrivono l'istituzione di dispositivi indipendenti di ricorso. Tali dispositivi possono assumere forme diverse, ma devono soddisfare le prescrizioni formulate nel contesto delle garanzie d'applicazione. Un'organizzazione può adempiere a tali prescrizioni nei modi seguenti: a) applicando programmi di riservatezza elaborati dal settore privato nei quali siano integrati i principi dell'approdo sicuro e che contemplino dispositivi di attuazione efficaci, del tipo descritto dal principio delle garanzie d'applicazione; 2) uniformandosi a norme giurisdizionali o regolamentari emanate dalle corrspondenti autorità di controllo, che disciplinino il trattamento di reclami individuali e la soluzione delle controversie; oppure 3) impegnandosi a cooperare con le autorità di tutela dei dati aventi sede nella Comunità europea o loro rappresentanti autorizzati. Quest'elenco è fornito a titolo puramente esemplificativo e non limitativo. Il settore privato può indicare altri meccanismi di applicazione, purchè rispettino il principio delle garanzie d'applicazione e le FAQ. Si noti che le citate garanzie d'applicazione si aggiungono a quelle di cui al paragrafo 3 dell'introduzione ai principi, in forza delle quali le iniziative di autoregolamentazione devono avere carattere vincolante in virtù dell'articolo 5 del Federal Trade Commission Act o analogo testo di legge.

Meccanismi di ricoso:

I consumatori dovrebbero essere incoraggiati a presentare gli eventuali reclami all'organizzazione direttamente interessata, prima di rivolgersi ai dispositivi indipendenti di ricorso. L'indipendenza di un dispositivo di ricorso è un dato di fatto che può essere dimostrato in vari modi, facendo valere ad esempio la trasparenza della composizione e del finanziamento oppure una comprovata esperienza. Come prescritto dal principio delle garanzie d'applicazione

il dispositivo di ricorso per i casi individuali deve essere di rapida fruizione e di costo non elevato. Gli organismi preposti alla soluzione dei contenziosi dovrebbero esaminare ogni reclamo presentato dai singoli, a meno che non si tratti di reclami chiaramente futili o infondati. Questo non pregiudica la definizione di criteri d'ammissibilità dei ricorsi da parte dell'organismo responsabile, ma tali criteri devono essere trasparenti e giustificati (ad esempio, esclusione di reclami che esulino dal campo d'applicazione del programma o siano di competenza di una diversa giurisdizione) e non devono andare a scapito dell'impegno di esaminare i ricorsi legittimi. I dispositivi di ricorso dovrebbero inoltre fornire alle persone che presentino un reclamo informazioni complete e pronte sul funzionamento della procedura di soluzione dei contenziosi. Di tali informazioni dovrebbero far parte accenni alle pratiche seguite in fatto di riservatezza nell'ambito dei dispositivi, conformemente ai principi dell'approdo sicuro (4). In tale contesto per semplificare il processo di gestione dei reclami sarebbe opportuno cooperare all'elaborazione di strumenti quali moduli di reclamo standard.

Riparazioni e sanzioni:

Le riparazioni ottenute tramite un organismo preposto alla soluzione delle controversie dovrebbero correggere o eliminare, nei limiti del possibile, gli effetti del mancato rispetto dei principi e fornire all'interessato la garanzia che in futuro l'organizzazione in questione tratterà i dati che lo riguardano nel rispetto di tali principi, ovvero cesserà di trattarli. Le sanzioni devono essere sufficientemente rigorose da garantire il rispetto dei principi. Una gamma di sanzioni di grado variabile consente di reagire in maniera proporzionale alla gravità delle infrazioni. Le sanzioni dovrebbero includere la pubblicazione del relativo verdetto ed eventualmente l'obbligo di cancellazione dei dati (5). Le sanzioni potrebbero comprendere la sospensione o il ritiro del «Marchio di conformità», il risarcimento degli eventuali danni, ed ingiunzioni. Se le loro decisioni non vengono rispettate, gli organismi per la risoluzione delle controversie e quelli di autoregolamentazione del settore privato devono notificare i tribunali o gli enti governativi competenti, nonchè il Dipartimento del commercio (o chi da esso designato).

Attività della Commissione federale per il commercio (Federal Trade Commission, FTC):

La Commissione federale per il commercio (FTC) se è impegnata ad esaminare in via prioritaria i casi trasmessi da organizzazioni di autoregolamentazione in materia di riservatezza (quali BBBOnline e TRUSTe) e dagli Stati membri dell'UE per denunciare la presunta non conformità ai principi dell'approdo sicuro, al fine di stabilire se vi siano state violazioni della sezione 5 del FTC Act, che vieta azioni o pratiche sleali od ingannevoli nel commercio. Se la FTC conclude che vi è motivo di ritenere che vi sia stata infrazione alle disposizioni della citata sezione 5, essa potrà risolvere il caso cercando di ottenere un ordine amministrativo di cessare e desistere che vieti le pratiche in questione, oppure presentando al tribunale distrettuale federale un reclamo che, se accolto, comporterebbe un'ordinanza del tribunale federale volta ad ottenere lo stesso effetto. La FTC può imporre ammende per violazioni di un ordine amministrativo di cessare e desistere e può perseguire in ambito civile o penale per mancato rispetto dell'autorità guidiziaria (contempt) l'inosservanza dell'ordine di un tribunale federale. La FTC notificherà qualsiasi azione essa decida di avviare al Dipartimento del commercio, che incoraggia altri organismi governativi ad informarlo dell'esito definitivo di qualsiasi caso ad essi deferito o di altre decisioni in tema di rispetto dei principi dell'approdo sicuro.

Inosservanza persistente:

L'organizzazione che persiste nel non rispettare i principi perde la facoltà di beneficiare dell'approdo sicuro. La fattispecie dell'inosservanza persistente si configura laddove un'organizzazione che abbia fornito l'autocertificazione al Dipartimento del commercio (od alla persona fisica o giuridica da esso designata) si rifiuti di uniformarsi a quanto deciso in ultima istanza da qualsiasi organismo governativo o di autoregolamentazione, o qualora tali organismi dichiarino che un'organizzazione infrange i principi con tale frequenza da togliere ogni creditibilità alle sue affermazioni formali di rispetto. In queste circostanze l'organizzazione è tenuta a notificare prontamente il Dipartimento del commercio (o chi da esso designato). La mancata notifica è perseguibile in forza del False Statements Act.

Il Dipartimento (o chi da esso designato) inserisce nell'elenco pubblico delle organizzazioni che autocertificano la propria conformità all'approdo sicuro qualsiasi notifica ricevuta in tal senso dall'organizzazione stessa, da organismi di autoregolamentazione o da organizzazioni governativi. Ciò avviene dietro preavviso all'organizzazione in questione, con possibilità di replica entro trenta giorni. L'elenco pubblico aggiornato dal Dipartimento del commercio (o chi da esso designato) permette così di stabilire quali organizzazioni possono beneficiare dell'approdo sicuro.

---

(4) Gli organismi preposti alla soluzione dei contenziosi non sono tenuti ad adeguarsi al principio delle garanzie d'applicazione. Nell'espletamento delle loro mansioni specifiche essi possono altresì derogare ai principi qualora incontrino obblighi contrastanti fra loro o autorizzazioni esplicite.

(5) Gli organismi preposti alla soluzione dei contenziosi dispongono di un margine di discrezione per quanto riguarda le circostanze in cui applicare tali sanzioni. La sensibilità dei dati in questione costituisce uno degli elementi da prendere in considerazione per decidere se richiederne la cancellazione, alla pari del fatto che un'organizzazione abbia raccolto, utilizzato o pubblicato informazioni contravvenendo in modo flagrante ai principi.

Un'organizzazione che chieda di partecipare ad un programma gestito da un organismo di autoregolamentazione al fine di riqualificarsi per l'approdo sicuro è tenuta a presentare a tale organismo tutte le informazioni relative alla sua precedente partecipazione all'approdo sicuro.

**FAQ 12 — Principio della scelta — Quando ci si può opporre?**

D: *Il principio della possibilità di scelta può essere fatto valere solo all'inizio del rapporto, o in qualsiasi momento?*

R: In generale il principio della possibilità di scelta ha lo scopo di garantire che le informazioni personali vengano utilizzate ed eventualmente divulgate in termini compatibili con le previsioni e le decisioni degli interessati. Di conseguenza i cittadini dovrebbero poter esercitare in qualsiasi momento la facoltà di scelta (od il diritto di opporsi o «opt-out») in rapporto all'impiego delle informazioni personali che li riguardano a fini di marketing diretto, subordinatamente al rispetto di limiti ragionevoli stabiliti dall'organizzazione, concernenti ad esempio il tempo necessario per dar seguito alla decisione. Un'organizzazione ha inoltre la facoltà di richiedere le informazioni necessarie per confermare l'identità del richiedente. Negli Stati Uniti le persone hanno la possibilità di esercitare quest'opzione servendosi di un servizio centrale come il Mail Preference Service della Direct Marketing Association. Le organizzazioni che partecipano a tale servizio dovrebbero pubblicizzarne l'esistenza presso i consumatori che non desiderano ricevere informazioni commerciali. In ogni caso ci si deve poter avvalere di un meccanismo prontamente disponibile a costi accessibili per esercitare quest'opzione.

Analogamente un'organizzazione può utilizzare informazioni per talune attività di marketing diretto ove non sia praticamente possibile dare all'individuo la possibilità di ritirarsi prima dell'utilizzo delle informazioni, purché al tempo stesso (e, su richista, in qualsiasi momento) l'organizzazione accordi prontamente all'interessato la possibilità di rifiutare (senza che ciò comporti alcun costo per lui) qualsiasi ulteriore comunicazione di marketing diretto e successivamente rispetti tale rifiuto.

**FAQ 13 — Informazioni relative ai viaggiatori**

D: *Quando è lecito trasferire ad organizzazioni ubicate al di fuori dell'UE informazioni ricavate da prenotazioni per voli o viaggi d'altro tipo, come ad esempio informazioni relative alla categoria dei frequent flyers o a particolare esigenze dei viaggiatori come precetti religiosi da rispettare in materia di pasti o necessità di assistenza materiale?*

R: Il trasferimento d'informazioni di questo genere è consentito in tutta una serie di circostanze differenti. A norma dell'articolo 26 della direttiva è lecito trasferire dati personali in «un paese terzo che non garantisce una tutela adeguata ai sensi dell'articolo 25, paragrafo 2» purché 1) ciò risulti necessario per l'esecuzione del contratto di trasporto e/o di stipulazioni del tipo frequent flyer, ovvero 2) l'interessato abbia manifestato il proprio consenso in maniera inequivocabile. Le organizzazioni statunitensi che abbiano aderito all'approdo sicuro garantiscono un'adeguata tutela dei dati personali e sono quindi abilitate a ricevere trasferimenti di dati dall'UE senza dover soddisfare dette condizioni od altre stabilite dall'articolo 26 della direttiva. L'impostazione dell'approdo sicuro dispone norme specifiche per le informazioni sensibili (la cui raccolta può risultare necessaria ad esempio in rapporto alle esigenze dei clienti in fatto d'assistenza materiale), cosicché queste possono far parte dei dati trasferiti ad organizzazioni che abbiano aderito all'approdo sicuro. L'organizzazione che provvede al trasferimento deve tuttavia uniformarsi in ogni caso alla normativa vigente nello Stato membro in cui opera, il quale può tra l'altro prescrivere condizioni speciali per il trasferimento di dati di natura sensibile.

**FAQ 14 — Medicinali e prodotti farmaceutici**

D 1: *Qualora dati personali vengano raccolti nell'UE e trasferiti negli Stati Uniti per la ricerca farmaceutica e/o altri fini, si applicano i principi dell'approdo sicuro oppure le disposizioni legislative degli Stati membri?*

R 1: Le disposizioni legislative degli Stati membri si applicano alla raccolta dei dati personali in questione e relativa elaborazione prima del trasferimento negli Stati Uniti. I principi dell'approdo sicuro si applicano ai dati quando vengono trasferiti negli Stati Uniti. I dati utilizzati per ricerche farmaceutiche e altri fini, all'occorrenza, dovrebbero essere resi anonimi.

D 2: *I dati personali acquisiti in campi specifici della ricerca medica o farmaceutica svolgono spesso un ruolo importante in future ricerche scientifiche. Quando i dati personali raccolti per uno studio vengono trasferiti a un'organizzazione statunitense nel quadro dell'approdo sicuro, può tale organizzazione utilizzare i dati per nuove attività di ricerca?*

R 2: Sì, qualora abbia in primo luogo dato adeguatamente avviso di tale intenzione ed abbia dato possibilità di scelta. Nell'informativa dovrebbero figurare informazioni concernenti tutte le future utilizzazioni dei dati, quali controlli periodici, studi correlati o marketing. È ovviamente impossibile specificare tutte le future utilizzazioni dei dati, poiché un nuovo impiego per la ricerca potrebbe rivelarsi necessario in seguito a nuovi studi sui dati originari, a scoperte e progressi della medicina, nonché a nuovi sviluppi della regolamentazione e della sanità pubblica. Se dunque il caso specifico lo richiede, nella informativa va indicato chiaramente che i dati personali possono essere utilizzati in future attività di ricerca medica e farmaceutica non preventivate. Qualora l'uso dei dati non sia compatibile con i fini generali della ricerca per cui essi sono stati originariamente raccolti o per cui la persona interessata aveva successivamente dato il suo consenso, è necessario ottenere un nuovo consenso.

D 3: *Qualora un partecipante decida volontariamente o su richiesta dell'ente promotore della ricerca di ritirarsi da una sperimentazione clinica, cosa avviene dei dati relativi?*

R 3: I partecipanti possono decidere di ritirarsi da una sperimentazione clinica, o essere invitati a farlo, in qualsiasi momento. I dati raccolti prima che il paziente si ritiri dalla sperimentazione possono essere ancora elaborati insieme agli altri dati raccolti nel corso della sperimentazione, purché tale possibilità sia stata segnalata al partecipante quando ha accettato di partecipare.

D 4: *Per motivi di regolamentazione e di supervisione le aziende produttrici di farmaci e di apparecchiature mediche possono fornire a enti regolatori statunitensi dati personali relativi a sperimentazioni cliniche condotte nell'UE. Simili trasferimenti possono essere fatti anche a parti terze, quali le filiali delle aziende o altri ricercatori?*

R 4: Sì, conformemente ai principi della informativa e della scelta.

D 5: *In molte sperimentazioni cliniche, per garantire l'obiettività, i partecipanti e sovente anche gli sperimentatori non possono avere accesso a informazioni relative al tipo di cura a cui ogni partecipante viene sottoposto, poiché in tal modo la validità della ricerca e dei relativi risultati verrebbe compromessa. I partecipanti a tali sperimentazioni cliniche (denominate «esperimenti in cieco») avranno accesso ai dati relativi al trattamento che ricevono durante la sperimentazione?*

R 5: No. Non vi è obbligo di accordare ad un partecipante tale accesso se questa restrizione è stata indicata esplicitamente al momento in cui la sperimentazione ha avuto inizio. La divulgazione di tali informazioni comprometterebbe inoltre l'integrità dell'intera ricerca. Il consenso a partecipare alla sperimentazione a queste condizioni è una ragionevole rinuncia al diritto di accesso. In seguito alla conclusione della sperimentazione ed all'analisi dei risultati i partecipanti devono poter accedere ai propri dati, qualora ne facciano richiesta. A tale scopo dovranno rivolgersi in primo luogo al medico o all'addetto del settore sanitario da cui sono stati curati durante la sperimentazione clinica oppure all'ente promotore della ricerca.

D 6: *Un'azienda produttrice di farmaci o di apparecchiature mediche è tenuta ad aderire ai principi dell'approdo sicuro per quanto riguarda informativa, scelta, trasferimento successivo ed accesso in relazione alle attività di sicurezza e controllo dei suoi prodotti, comprese la segnalazione di eventi sfavorevoli e l'assistenza ai pazienti/soggetti che utilizzano particolari medicinali o apparecchiature mediche (ad esempio un pacemaker)?*

R 6: No, nella misura in cui l'applicazione dei principi dell'approdo sicuro interferisce con il rispetto delle regolamentazioni. Questo vale sia per le segnalazioni fatte ad esempio da un addetto del settore sanitario alle aziende produttrici di farmaci e di apparecchiature mediche, sia per le segnalazioni fatte da tali aziende ad enti governativi, quali la Food and Drug Administration (l'organismo di controllo degli alimenti e dei farmaci).

D 7: *Per non rivelare l'identità dei singoli partecipanti lo sperimentatore principale assegna invariabilmente ai dati della ricerca un codice di accesso unico. Le aziende farmaceutiche che promuovono tale ricerca non ricevono il codice di accesso. Soltanto il ricercatore ne è in possesso per poter essere in grado d'identificare il partecipante in circostanze particolari (ad esempio quando è necessario un supplemento d'assistenza medica). Un trasferimento dall'UE agli Stati Uniti di dati codificati in questo modo costituisce un trasferimento di dati personali soggetto ai principi dell'approdo sicuro?*

R 7: No; questo modo di procedere non costituisce un trasferimento di dati personali soggetto ai principi in questione.

**FAQ 15 — Informazioni pubbliche e di dominio pubblico**

D: *I principi di informativa, scelta, e successivo trasferimento vanno applicati anche alle informazioni che figurano in archivi e registri pubblici o sono comunque di pubblico dominio?*

R: Non occorre applicare i principi di informativa, scelta o successivo trsferimento alle informazioni a carattere pubblico, a meno che non comprendano anche elementi non di pubblico dominio, e vengano rispettate le condizioni eventualmente stabilite per la consultazione dalla competente giurisdizione.

Parimenti, di norma non è necessario applicare i principi di informativa, scelta o successivo trasferimento ad informazioni di pubblico dominio, a meno che il trasferente europeo non indichi che le informazioni in questione sono soggette a restrizioni che comportano l'obbligo per l'organizzazione interessata di applicare tali principi. Le organizzazioni non sono responsabili dell'uso di siffatte informazioni da parte di chi le abbia ricavate da fonti pubblicate.

Qualora risulti che un'organizzazione abbia deliberatamente divulgato informazioni aventi carattere personale in violazione ai principi per trarre beneficio, o consentire a terzi di trarre beneficio, dalle eccezioni di cui sopra, l'organizzazione cessa di qualificarsi per l'approdo sicuro.

*ALLEGATO III*

## Applicazione (enforcement) dell'approdo sicuro

### Autorità statale e federale in materia di «pratiche sleali e ingannevoli» e riservatezza

Il presente memorandum illustra sinteticamente l'autorità della Federal Trade Commission (FTC) ai sensi della sezione 5 del Federal Trade Commission Act (15 U.S.C., §§ 41-58, con emendamenti) nei confronti di istanze che vengano meno all'obbligo di proteggere la riservatezza delle informazioni personali in conformità ad impegni presi e/o dichiarazioni effettuate. Vengono discusse anche le eccezioni a tale autorità, e la possibilità di altri enti statali e federali di intervenire nei casi in cui l'FTC non possiede tale facoltà ([1]).

### Autorità dell'FTC in materia di pratiche sleali o ingannevoli

La sezione 5 del Federal Trade Commission Act dichiara illegali «le attività o le pratiche sleali o ingannevoli in materia commerciale o collegata al commercio», cfr. 15 U.S.C. § 45(a)(1). La sezione 5 conferisce all'FTC poteri plenari per prevenire tali atti e pratiche, cfr. 15 U.S.C. § 45(a)(2). Per conseguenza, l'FTC ha facoltà, previa udienza formale, di emanare ordinanze di «cessare e desistere» al fine di porre termine alle violazioni, cfr. 15 U.S.C. § 45(b). Per motivi d'interesse pubblico, l'FTC ha inoltre facoltà di sollecitare un'ordinanza temporanea o un'ingiunzione temporanea o permanente da parte di un tribunale distrettuale degli Stati Uniti, cfr. 15 U.S.C. § 53(b). Qualora vi sia una situazione di ampia diffusione degli atti o pratiche sleali o ingannevoli, o qualora abbia già formulato ordinanze di cessare e desistere in materia, l'FTC ha facoltà di promulgare norme amministrative tali da coprire gli atti o pratiche in questione, cfr. 15 U.S.C. § 57a.

Chiunque non rispetti le ordinanze dell'FTC è soggetto ad una sanzione civile fino a un massimo di 11 000 USD, con ciascun giorno in cui la violazione continua costituente violazione separata ([2]), cfr. 15 U.S.C. § 45(1). Allo stesso modo, chiunque infranga scientemente una regola dell'FTC è passibile di una penale di 11 000 USD per ciascuna violazione, cfr. 15 U.S.C. § 45(m). Le azioni volte ad ottenere l'ottemperanza possono essere intraprese dal Dipartimento della giustizia o in alternativa dall'FTC, cfr. 15 U.S.C. § 56.

### Autorità dell'FTC e riservatezza

Nell'esercizio dell'autorità che le compete ai sensi della citata sezione 5, l'FTC parte dal presupposto che ogni rappresentazione ingannevole dei motivi per cui le informazioni vengono raccolte dai consumatori, o del modo in cui le informazioni saranno utilizzate, costituisce pratica ingannevole ([3]). Ad esempio, nel 1998 l'FTC ha iniziato un procedimento nei confronti della GeoCities per divulgazione a terzi, a fini di sollecitazione commerciale e senza precedente autorizzazione, di informazioni raccolte sul proprio sito Web nonostante dichiarazioni contrarie ([4]). Il personale dell'FTC ritiene inoltre che la raccolta di informazioni personali presso minori, e la vendita e divulgazione di tali informazioni senza il consenso dei genitori, costituisca probabilmente pratica sleale ([5]).

---

([1]) Non vengono discussi in questa sede tutti i vari statuti federali che interessano questioni di riservatezza in contesti specifici, e neppure tutti gli statuti statali o altre disposizioni della Common Law che potrebbero essere applicabili. Gli statuti a livello federale che regolano la raccolta e l'impiego a fini commerciali di informazioni personali comprendono il Cable Communications Policy Act (47 U.S.C. § 551), il Driver's Privacy Protection Act (18 U.S.C. § 2721), l'Electronic Communications Privacy Act (18 U.S.C. § 2701 et seq.), l'Eletronic Funds Transfer Act (15 U.S.C. §§ 1693, 1693m), il Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.), il Right to Financial Privacy Act (12 U.S.C. § 3401 et seq.), il Telephone Consumer Protection Act (47 U.S.C. § 227), e il Video Privacy Protection Act (18 U.S.C. § 2710), fra gli altri. Numerosi stati hanno approvato analoghe disposizioni di legge in questi settori. Cfr. ad esempio Mass. Gen. Laws ch. 167B. § 16 (che proibisce alle istituzioni finanziarie di fornire a terzi informazioni finanziarie sui clienti senza il consenso degli stessi, o debito procedimento legale), N.Y. Pub. Health Law § 17 (che limita l'impiego e la comunicazione delle informazioni mediche o in materia di salute mentale, e stabilisce il diritto dei pazienti di avere accesso a tali informazioni).

([2]) In tal caso, il tribunale distrettuale degli Stati Uniti può inoltre impartire disposizioni o ingiunzioni al fine di assicurare il rispetto dell'ordinanza dell'FTC, cfr. 15 U.S.C. § 45(1).

([3]) «Pratica ingannevole» viene definita come una rappresentazione, omissione o pratica destinata probabilmente a trarre materialmente in inganno consumatori ragionevoli.

([4]) Cfr. www.ftc.gov/opa/1998/9808/geocitie.htm.

([5]) Cfr. lettera al Center for Media Education, www.ftc.gov/os/1997/9707/cenmed.htm. Inoltre, il Children's Online Privacy Protection Act del 1998 conferisce all'FTC specifica autorità di legge per regolare la raccolta di informazioni personali presso minori ad opera di operatori di siti Web e di servizi on-line. Cfr. 15 U.S.C. §§ 6501-6506. In particolare, la legge citata obbliga gli operatori online ad effettuare avvertenze e ad ottenere un consenso verificabile dei genitori prima di raccogliere, utilizzare o divulgare informazioni personali provenienti da minori. Ibidem, § 6502(b). Questa legge conferisce inoltre ai genitori un diritto d'accesso e di divieto della prosecuzione dell'uso delle informazioni. Ibidem.

In una lettera al direttore generale John Mogg della Commissione europea, il presidente dell'FTC Pitofsky ha indicato i limiti dell'autorità dell'FTC in materia di protezione della riservatezza in assenza della fattispecie di dichiarazioni sleali o ingannevoli (o di alcuna dichiarazione) sulla destinazione delle informazioni raccolte. Lettera del presidente dell'FTC Pitofsky a John Mogg (23 settembre 1998). Tuttavia, le imprese che intendono avvalersi del proposto «approdo sicuro» devono dichiarare l'intenzione di proteggere le informazioni raccolte in conformità ai principi fissati. Per conseguenza, se un'impresa certifica la propria intenzione di salvaguardare la riservatezza delle informazioni e poi viene meno a tale impegno, il fatto costituisce «pratica ingannevole» ai sensi della sezione 5.

Dato che la giurisdizione dell'FTC è limitata agli atti o pratiche sleali o ingannevoli «in materia commerciale o collegata al commercio», l'FTC non è competente per quanto riguarda la raccolta e impiego di informazioni personali a fini non commerciali, ad esempio raccolta di fondi per attività caritatevoli, cfr. lettera Pitofsky, pag. 3. Tuttavia, l'utilizzazione di informazioni personali in qualsiasi transazione a carattere commerciale è tale da soddisfare il citato requisito giurisdizionale. In tal modo, ad esempio, la vendita da parte di un datore di lavoro a un'impresa di marketing diretto di informazioni personali sui dipendenti rientra nell'ambito della sezione 5.

**Eccezioni alla sezione 5**

La sezione 5 definisce le seguenti eccezioni all'autorità dell'FTC in materia di atti o pratiche sleali o ingannevoli:

— istituzioni finanziarie, comprese banche, casse di risparmio e unioni di credito;

— vettori comuni di telecomunicazione e di trasporti interstatali;

— vettori aerei;

— operatori del settore zootecnico (macellazione, trasformazione e commercio all'ingrosso).

Cfr. 15 U.S.C. § 45(a)(2). Esaminiamo ora tali eccezioni e le relative autorità competenti.

*Istituti finanziari* (6)

La prima eccezione interessa le «banche, casse di risparmio e istituti di credito di cui alla sezione 18(f)(3)[15 U.S.C. § 57a(f)(3)]» e «le unioni federali di credito di cui alla sezione 18(f)(4) [15 U.S.C. § 57a(f)(4)]» (7). Queste istituzioni finanziarie sono invece soggette ai regolamenti emanati dal Federal Reserve Board, dall'Office of Thrift Supervision (8) e dal National Credit Union Administration Board, cfr. 15 U.S.C. § 57a(f). Questi organi hanno facoltà di prescrivere i regolamenti necessari per impedire pratiche sleali e ingannevoli da parte di queste istituzioni finanziarie (9) e di istituire appositi dipartimenti allo scopo di accogliere i ricorsi del pubblico, cfr. 15 U.S.C. § 57a(f)(1). Infine, l'opportuna autorità esecutiva deriva dalla sezione 8 del Federal Deposit Insurance Act (12 U.S.C. § 1818) per quanto riguarda le banche e le casse di risparmio, e dalle sezioni 120 e 206 del Federal Credit Union Act per quanto riguarda le unioni federali di credito, cfr. 15 U.S.C. §§ 57a(f)(2)-(4).

Benché l'industria assicurativa non sia specificatamente compresa nell'elenco delle eccezioni alla sezione 5, il McCarran-Ferguson Act (15 U.S.C. § 1011 et seq.) in generale demanda la regolamentazione delle attività assicurative

(6) Il 12 novembre 1999 il Presidente Clinton ha promulgato il Gramm-Leach-Bliley Act (Pub. L. 106-102, codificato in 15 U.S.C. § 6801 et seq.). Tale atto limita la rivelazione da parte di istituti finanziari di informazioni personali sui loro clienti. È previsto che gli istituti finanziari, fra l'altro, notifichino a tutti i clienti le rispettive politiche e pratiche in materia di riservatezza per quanto attiene alla trasmissione di informazioni personali ad affiliati e non affiliati. La legge autorizza l'FTC, le autorità federali del settore bancario ed altre autorità a promulgare regolamenti per l'applicazione delle previste misure per la tutela della riservatezza. Questi enti hanno pubblicato i regolamenti previsti allo scopo.

(7) In virtù della maniera in cui è formulata, questa eccezione non si applica al settore dei titoli. Pertanto, gli agenti e altri operatori di borsa sono soggetti alla contemporanea giurisdizione dell'FTC e della Securities and Exchange Commission per quanto riguarda atti e pratiche sleali o ingannevoli.

(8) L'eccezione alla sezione 5 si riferiva in origine al Federal Home Loan Bank Board che è stato abolito nell'agosto 1989 dal Financial Institutions Reform, Recovery and Enforcement Act. Le sue funzioni sono state trasferite all'Office of Thrift Supervision, alla Resolution Trust Corporation, alla Federal Deposit Insurance Corporation, e all'Housing Finance Board.

(9) Pur sottraendo gli istituti finanziari alla giurisdizione dell'FTC, la sezione 5 prevede anche che qualora l'FTC promulghi una norma in materia di atti e pratiche sleali o ingannevoli, gli organi di regolamentazione del settore finanziario devono adottare analoghi regolamenti entro 60 giorni, cfr. 15 U.S.C. § 57a(f)(1).

ai singoli stati ([10]). Inoltre, ai sensi della sezione 2(b) del McCarran-Ferguson Act, nessuna legge federale può invalidare, infirmare o sostituire regolamenti emessi dagli stati «salvo il caso che la legge in questione verta specificatamente sulle attività assicurative», cfr. 15 U.S.C. § 1012(b). Tuttavia, le disposizioni dell'FTC Act si applicano all'industria assicurativa «nella misura in cui tali attività non sono regolate da leggi statali». Ibidem. Merita rilevare, inoltre, che il McCarran-Ferguson Act statuisce tale preminenza degli stati soltanto per quanto riguarda le «attività assicurative». Pertanto, l'FTC rimane competente nel caso di pratiche sleali o ingannevoli da parte di società di assicurazione qualora tali società non siano impegnate in attività assicurative. Ciò potrebbe comprendere, ad esempio, il caso di assicuratori che vendono informazioni personali sui loro assicurati a imprese di marketing diretto di prodotti non assicurativi ([11]).

*Vettori comuni*

La seconda eccezione alla sezione 5 interessa i vettori comuni «soggetti ad atti per la regolazione del commercio», cfr. 15 U.S.C. § 45(a)(2). In questo caso, la formula «atti per la regolazione del commercio» si rifersice alla sezione IV del titolo 49 dell'United States Code ed al Communications Act del 1934 (47 U.S.C. § 151 et seq.) (Communications Act), cfr. 15 U.S.C. § 44.

Il 49 U.S.C. subtitle IV (Interstate Transportation) si applica ai vettori di trasporti su ferrovia, su strada, vie d'acqua, nonché intermediari, spedizionieri e vettori su pipeline, cfr. 49 U.S.C. § 10101 et seq. Tutti questi vettori sono soggetti ai regolamenti del Surface Transportation Board, un ente indipendente in seno al Dipartimento dei trasporti, cfr. 49 U.S.C. §§ 10501, 13501, e 15301. In tutti questi casi, si fa divieto al vettore di rivelare informazioni sulla natura, destinazione ed altri aspetti del carico che potrebbero essere utilizzate a danno del mittente, cfr. 49 U.S.C. §§ 11904, 14908, e 16103. Merita rilevare che queste disposizioni si riferiscono a informazioni concernenti il carico, e non sembra che possano comprendere informazioni personali sul mittente che non siano collegate alla spedizione di un carico.

Per quanto riguarda il Communications Act, tale testo prevede la regolazione del «commercio interstatale ed estero in comunicazioni su filo e via radio» da parte della Federal Communications Commission (FCC), cfr. 47 U.S.C. §§ 151 e 152. Oltre ai vettori comuni delle telecomunicazioni, il Communications Act si applica anche a imprese quali emittenti radio e televisive e fornitori di servizi via cavo che non siano vettori comuni. In quanto tali, queste ultime imprese non sono qualificate per rientrare nell'eccezione alla sezione 5 dell'FTC Act. Pertanto, l'FTC è competente per perseguire tali società in caso di pratiche sleali e ingannevoli, mentre l'FCC è contemporaneamente competente per l'esecuzione della propria autorità indipendente in questo settore, come illustrato in appresso.

In base al Communications Act, «qualsiasi vettore di telecomunicazioni» compresi i vettori locali, ha il dovere di proteggere la riservatezza delle informazioni proprie dei clienti ([12]), cfr. 47 U.S.C. § 222(a). Oltre a questa generale competenza in materia di protezione della riservatezza, il Communications Act è stato emendato dal Cable Communcations Policy Act del 1984 (the Cable Act), cfr. 47 U.S.C. § 521 et seq., per disporre espressamente l'obbligo per gli operatori via cavo di tutelare la riservatezza di «informazioni identificabili personalmente» sugli abbonati a tali servizi, cfr. 47 U.S.C. § 551 ([13]). Il Cable Act limita la raccolta d'informazioni personali da parte degli operatori via cavo, e prevede che tali operatori notifichino agli abbonati la natura delle informazioni raccolte e il modo in cui tali informazioni saranno utilizzate. Il Cable Act stabilisce che gli abbonati hanno diritto di accesso alle informazioni che li riguardano, e fa obbligo agli operatori via cavo di distruggere tali informazioni quando non sono più necessarie.

Il Communications Act autorizza l'FCC ad assicurare l'esecuzione di queste due disposizioni in materia di riservatezza, sia di propria iniziativa che in risposta ad un reclamo proveniente dall'esterno ([14]), cfr. 47 U.S.C. §§ 205, 403; ibidem § 208. Se l'FCC determina che un vettore di telecomunicazione (compresi gli operatori via cavo) ha infranto le disposi-

([10]) «The business of insurance, and every person engaged therein, shall be subject to the laws of the several States which relate to the regulation or taxation of such business», cfr. 15 U.S.C. § 1012(a).

([11]) L'FTC ha esercitato giurisdizione su società assicurative in diversi contesti. In un caso, l'FTC è intervenuta nei confronti di una società a causa di pubblicità ingannevole in uno stato in cui tale società non disponeva di autorizzazione allo svolgimento di attività commerciali. La giurisdizione dell'FTC è stata confermata dal tribunale in quanto non sussisteva alcun regolamento statale applicabile dato che l'impresa di fatto si trovava al di fuori della giurisdizione dello stato in questione, cfr. FTC v. Travelers Health Association, 362 U.S. 293 (1960).
Per quanto riguarda gli stati, diciassette di essi hanno adottato il modello «Insurance Information and Privacy Protection Act» della National Association of Insurance Commissioners (NAIC). Tale atto comprende disposizioni in materia di avviso, utilizzazione, divulgazione e accesso. Inoltre, quasi tutti gli stati hanno adottato il modello NAIC «Unfair Insurance Practices Act», che verte espressamente sulle pratiche commerciali sleali nell'industria assicurativa.

([12]) Per «informazioni di rete proprie dei clienti» si intendono le informazioni relative «alla quantità, configurazione tecnica, tipo, destinazione e impiego di un servizio di telecomunicazione» da parte di un cliente, nonché informazioni in materia di fatturazione telefonica, cfr. 47 U.S.C. § 222(f)(1). Tuttavia, non sono comprese le informazioni in materia di elenchi di abbonamento. Ibidem.

([13]) La legislazione non definisce espressamente il concetto di «informazioni identificabili personalmente».

([14]) Tale autorità comprende il diritto di rimedio giuridico (redress) per violazioni della riservatezza ai sensi della sezione 222 del Communications Act ovvero, per quanto riguarda gli abbonati a servizi via cavo, della sezione 551 dell'emendamento a tale atto mediante il Cable Act. Cfr. anche 47 U.S.C. § 551(f)(3) (l'azione civile in un tribunale distrettuale federale costituisce un rimedio non esclusivo, offerto «in aggiunta a qualsiasi altro legittimo rimedio disponibile a un abbonato via cavo»).

zioni sulla riservatezza di cui alla sezione 222 o alla sezione 551, essa può intraprendere tre azioni diverse. Primo, previa udienza e verdetto di infrazione, la Commissione può ordinare la vettore di versare indennizzi pecuniari ([15]), cfr. 47 U.S.C. § 209. Alternativamente, l'FCC può ordinare la vettore di cessare e desistere dalla pratica o dall'omissione in questione, cfr. 47 U.S.C. § 205(a). Infine, tale Commissione ha facoltà di ordinare al vettore di «conformarsi e osservare [qualsiasi] regolamento o pratica», che l'FTC possa prescrivere. Ibidem.

Un privato cittadino che ritiene che un vettore di telecomunicazioni o un operatore via cavo abbia infranto le pertinenti disposizioni del Communications Act o del Cable Act può presentare un ricorso all'FCC o adire direttamente a un tribunale distrettuale federale, cfr. 47 U.S.C. § 207. Il ricorrente la cui azione contro un vettore di telecomunicazioni per mancata protezione di informazioni proprietarie dei clienti ai sensi della sezione 222 del Communications Act venga accolta da un tribunale federale può ricevere un indennizzo per i danni subiti e le spese per onorari, cfr. 47 U.S.C. § 206. Il ricorrente che intraprenda un'azione per violazione della riservatezza in base alla sezione 551 del Cable Act, limitata agli operatori via cavo, può ricevere, oltre ai danni effettivi e alle spese per onorari, anche un importo per danni punitivi e per ragionevoli costi della procedura, cfr. 47 U.S.C. § 551(f).

L'FCC ha adottato norme particolareggiate per l'applicazione della sezione 222, cfr. 47 CFR 64.2001-2009. Tali norme stabiliscono specifiche salvaguardie di tutela per casi di accesso non autorizzato a informazioni di rete di proprietà dei clienti. I regolamenti prevedono i seguenti obblighi per i vettori delle telecomunicazioni:

— sviluppo e implementazione di sistemi software per la segnalazione automatica («flag») dell'avviso/approvazione del cliente quando i relativi dati compaiono per la prima volta sullo schermo;

— mantenimento di una «traccia elettronica» che permetta di controllare l'accesso alle informazioni relative a un cliente, ed in particolare chi, quando e perché ha avuto accesso alle informazioni su un cliente;

— formazione del personale in materia di impiego autorizzato di informazioni di rete di proprietà dei clienti, con istituzione di opportune procedure disciplinari;

— istituzione di un processo di revisione e supervisione per garantire il rispetto della riservatezza nel caso dell'effettuazione di attività di marketing esterne;

— certificazione all'FCC su base annua del modo in cui vengono applicati i suddetti regolamenti.

*Vettori aerei*

I vettori aerei americani e stranieri soggetti al Federal Aviation Act del 1958 sono anch'essi esenti dalla Sezione 5 dell'FTC Act, cfr. 15 U.S.C. § 45(a)(2). Ciò comprende chiunque presti servizi di trasporto estero o interstatale di passeggeri o di merci, o che effettui trasporti postali, per via aerea, cfr. 49 U.S.C. § 40102. I vettori aerei sono soggetti all'autorità del Dipartimento dei trasporti. A questo proposito, il Segretario di tale Dipartimento ha facoltà di intraprendere azioni tali da prevenire pratiche anticompetitive, ingannevoli, sleali o predatorie nei trasporti aerei, cfr. 49 U.S.C. § 40101(a)(9). Il Segretario dei trasporti ha facoltà, qualora tali indagini siano nel pubblico interesse di indagare se un vettore aereo straniero o degli Stati Uniti, ovvero un agente di viaggio, abbia compiuto pratiche sleali o ingannevoli, cfr. 49 U.S.C. § 41712. Previa udienza, il Segretario dei trasporti ha facoltà di emanare un'ordinanza per porre termine alla pratica illecita, ibidem. Per quanto ci consta, il Segretario dei trasporti non ha esercitato tale autorità in ordine al problema della protezione della riservatezza delle informazioni personali dei passeggeri delle linee aeree ([16]).

Vi sono due disposizioni per la tutela della riservatezza delle informazioni personali che si applicano ai vettori aerei in contesti specifici. Primo, il Federal Aviation Act protegge la riservatezza dei candidati a compiti di pilotaggio, cfr. 49 U.S.C. § 44936(f). Mentre da un lato i vettori aerei hanno facoltà di ottenere il curriculum professionale di tali candidati, ogni candidato ha il diritto di essere avvertito che il suo curriculum è stato richiesto, di dare il suo consenso alla richiesta, di correggere eventuali inesattezze e di avere la certezza che le informazioni siano divulgate soltanto ai responsabili della decisione nel suo caso specifico. Secondo, i regolamenti del Dipartimento dei trasporti prevedono che le informazioni sugli elenchi dei passeggeri raccolte a fini amministrativi in caso di una sciagura «rimangano riservate e siano comunicate soltanto al Dipartimento di Stato degli Stati Uniti, al National Transportation Board (su richiesta), e al Dipartimento dei trasporti degli Stati Uniti», cfr. 14 CFR part 243, § 243.9(c) (integrato da 63 FR 8258).

([15]) L'assenza di un danno diretto a un ricorrente non costituisce peraltro un motivo per respingere un reclamo, cfr. 47 U.S.C. § 208(a).

([16]) Ci risulta che in seno all'industria dei trasporti aerei sono in corso sforzi per affrontare il problema della riservatezza. I rappresentanti dell'industria hanno discusso i proposti principi dell'approdo sicuro e la loro possibile applicazione ai trasporti aerei. Tale discussione ha compreso altresì una proposta per l'adozione di una politica dell'industria dei trasporti aerei in materia di riservatezza, in virtù della quale le imprese partecipanti si sottoporrebbero espressamente all'autorità del Dipartimento dei trasporti.

*Operatori del settore zootecnico (macellazione, trasformazione e commercio all'ingrosso)*

Per quanto riguarda il Packers and Stockyards Act del 1921 (7 U.S.C. § 181 et seq.), tale atto vieta che «qualsiasi operatore in bestiame vivo, carne macellata, prodotti alimentari a base di carne, o prodotti alimentari in forma non manifatturata, o qualsiasi grossista di pollame vivo per quanto riguarda il pollame vivo, effettui o si avvalga di qualsiasi pratica o dispositivo ingannevole, ingiustamente discriminatorio o sleale», cfr. 7 U.S.C. § 192(a); cfr. anche 7 U.S.C. § 213(a) (che proibisce «qualsiasi pratica o dispositivo ingannevole, inguistamente discriminatorio o sleale» in collegamento a bestiame vivo).

Il Segretario dell'agricoltura ha responsabilità primaria per quanto riguarda il rispetto di queste disposizioni, mentre l'FTC mantiene la propria giurisdizione sulle transazioni al dettaglio e su quelle relative all'avicoltura, cfr. 7 U.S.C. § 227(b)(2). Non è chiaro se il Segretario dell'agricoltura possa interpretare il mancato rispetto da parte dei suddetti operatori della riservatezza dei dati personali conformemente a precedenti dichiarazioni come una pratica «ingannevole» ai sensi del Packers and Stockyards Act. Tuttavia, l'eccezione alla sezione 5 si applica a persone, associazioni o società soltanto «nella misura in cui tali istanze sono soggette al Packers and Stockyards Act». Pertanto, se la riservatezza dei dati personali non rientra nell'ambito del Packers and Stockyards Act, allora l'eccezione alla sezione 5 potrebbe benissimo non sussistere e questi operatori sarebbero soggetti all'autorità dell'FTC a tale proposito.

**Autorità degli stati in materia di «pratiche ingannevoli e sleali»**

In base ad un'analisi effettuata da personale dell'FTC, «tutti i cinquanta stati più il distretto di Columbia, Guam, Puerto Rico, e le Isole Vergini degli Stati Uniti hanno promulgato leggi più o meno simili al Federal Trade Commission Act ("FTCA") per prevenire le pratiche commerciali sleali o ingannevoli», cfr. Bollettino FTC, in Comment, Consumer Protection: The Practical Effectiveness of State Deceptive Trade Practices Legislation, 59 Tul. L. Rev. 427 (1984). In tutti i casi un ente competente ha l'autorità «di effettuare indagini giudiziarie a carattere civile o penale, ottenere assicurazioni di volontaria ottemperanza, emanare ordinanze di cessare e desistere o sollecitare ingiunzioni della magistratura tali da prevenire l'impiego di pratiche commerciali ingannevoli, inique o sleali», ibidem. In 46 giurisdizioni, la legge ammette azioni private per danni effettivi, doppi, tripli o punitivi, e, in taluni casi, per il recupero delle spese legali e degli onorari, ibidem.

Nel caso della Florida, ad esempio, il Deceptive and Unfair Trade Practices Act autorizza l'Attorney General ad effettuare indagini e a promuovere azioni in sede civile in materia di «metodi sleali di concorrenza, pratiche commerciali ingannevoli, inique o sleali», compresa la pubblicità falsa o ingannevole, le pratiche ingannevoli in materia di franchising o di opportunità commerciali, le pratiche fraudolente in materia di telemarketing e le truffe cosiddette piramidali, cfr. anche N.Y. General Business Law § 349 (che proibisce gli atti sleali e le pratiche ingannevoli nel corso dell'attività commerciale).

Un'indagine dello scorso anno effettuata dalla National Association of Attorneys General (NAAG) ha confermato queste indicazioni. Su 43 stati che hanno inviato una risposta, tutti prevedono statuti tipo «mini FTC» ovvero norme che prevedono una tutela comparabile. Sempre secondo l'indagine NAAG, 39 stati hanno indicato l'esistenza di un'autorità a cui possono essere presentati ricorsi da parte di non residenti. Per quanto riguarda la riservatezza dei consumatori, in particolare, 37 dei 41 stati che hanno risposto hanno indicato che accoglierebbero ricorsi nei confronti di società con sede nella loro giurisdizione in caso di mancato rispetto di una politica dichiarata in fatto di riservatezza.

*ALLEGATO IV*

**Tutela della riservatezza e risarcimento danni, autorizzazioni legali, fusioni e acquisizioni secondo la legge degli Stati Uniti**

Il presente documento risponde alla richiesta della Commissione europea di chiarimenti sulla legge statunitense per quanto riguarda a) risarcimento dei danni per violazione della sfera privata (privacy), b) le «autorizzazioni esplicite» previste dalla legge degli Stati Uniti per l'uso di dati personali in modo contrastante con i principi «approdo sicuro» (safe harbor), c) l'effetto delle fusioni e acquisizioni sugli obblighi assunti in base a tali principi.

## A. **Risarcimento dei danni per violazione della privacy**

Il mancato rispetto dei principi «approdo sicuro» potrebbe provocare, secondo le circostanze, reclami da parte di privati. In particolare, le organizzazioni aderenti ai principi «approdo sicuro» potrebbero essere ritenute responsabili di falsa dichiarazione per non essersi attenute ai principi cui hanno dichiarato di conformarsi. La legge prevede inoltre la possibilità di intentare cause per il risarcimento dei danni conseguenti a violazioni della privacy. Molte disposizioni di legge federali e dei singoli Stati in materia di tutela della privacy, inoltre, prevedono per i privati la possibilità di chiedere il risarcimento dei danni derivanti da violazioni.

*Il diritto al risarcimento dei danni per violazione della privacy personale è ben definito dalla legge statunitense.*

Secondo varie teorie giuridiche, l'uso dei dati personali in modo contrastante con i principi «approdo sicuro» può dar luogo ad una responsabilità legale. Ad esempio, sia il responsabile del trasferimento dei dati, sia le persone interessate potrebbero citare in giudizio per falsa dichiarazione l'organizzazione aderente ai principi «approdo sicuro» che non rispetti gli impegni presi. Secondo Restatement of the Law, Second, Torts [1]:

> Chi fraudolentemente rilascia una falsa dichiarazione in merito a fatti, pareri, intenzioni o leggi allo scopo di indurre un'altra persona ad agire o a non agire sulla base di tale dichiarazione, è responsabile del danno pecuniario che questa persona abbia subito per aver prestato fede, per ragioni giusitificabili, alla falsa dichiarazione.

Restatement § 525. Una falsa dichiarazione è considerata «fraudolenta» se chi ne è l'autore è a conoscenza della sua falsità. Ibidem § 526. Di norma, l'autore di una falsa dichiarazione fraudolenta è potenzialmente responsabile nei confronti di chiunque egli ritiene o prevede che possa dar credito a tale falsa dichiarazione per ogni danno pecuniario da essa derivante. Ibidem § 531. Inoltre, chi rilascia ad altri una falsa dichiarazione fraudolenta può essere ritenuto responsabile nei confronti di terzi se ritiene o prevede che la sua falsa dichiarazione possa essere ripetuta a terzi e che questi possano agire in base ad essa. Ibidem § 533.

Nel contesto dell'approdo sicuro, la dichiarazione pertinente è la dichiarazione pubblica con la quale l'organizzazione s'impegna a conformarsi ai principi «approdo sicuro». Avendo assunto un tale impegno, un'inosservanza consapevole di quei principi potrebbe motivare un'azione legale per falsa dichiarazione promossa da quanti hanno prestato fede alla falsa dichiarazione. Poiché l'impegno ad attenersi ai principi è preso nei confronti del pubblico in generale, le persone interessate e i responsabili del trattamento in Europa che trasferiscono dati personali all'organizzazione statunitense potrebbero intraprendere un'azione legale nei confronti dell'organizzazione statunitense per falsa dichiarazione [2]. Inoltre, l'organizzazione statunitense rimane responsabile nei loro confronti per «falsa dichiarazione continuata» fintanto che questi prestano fede, con loro pregiudizio, alla falsa dichiarazione. Restatement, § 535.

[1] Second Restatement of the Law — Torts; American Law Institute (1997) (2. Bearbeitung der Rechtsgrundsätze, Sachgebiet unerlaubte Handlungen, Amerikanisches Rechtsinstitut).

[2] Questo potrebbe essere il caso, per esempio, delle persone che hanno dato il loro consenso al trasferimento negli Stati Uniti di dati personali confidando nell'impegno dell'organizzazione statunitense ad attenersi ai principi «approdo sicuro».

Chi presta fede ad una falsa dichiarazione fraudolenta ha diritto al risarcimento dei danni. Secondo il Restatement:

> Il destinatario della falsa dichiarazione fraudolenta ha diritto al risarcimento del danno pecuniario subito, in conseguenza della falsa dichiarazione.

Restatement, § 549. I danni risarcibili comprendono le perdite effettive oltre che il mancato guadagno in una trasazione commerciale. Ibidem; cfr., ad esempio, Boling v. Tennessee State Bank, 890 S.W.2d 32 (1994) (la banca è obbligata a risarcire ai mutuatari 14 825 USD per aver diffuso dati personali e piani d'impresa dei mutuatari al presidente della banca che aveva con loro un conflitto d'interessi).

Dato che la falsa dichiarazione fraudolenta implica la consapevolezza effettiva, o quanto meno la convinzione della falsità della dichiarazione, la responsabilità può anche essere estesa alla negligenza. Secondo Restatement, chiunque rilasci una falsa dichiarazione nel corso della sua attività, professione, o occupazione, o in una qualsiasi transazione pecuniaria, può essere ritenuto responsabile «per negligenza o incompetenza nell'ottenere o nel comunicare le informazioni». Restatement, § 552 (1). Contrariamente alle false dichiarazioni fraudolente, il risarcimento dei danni subiti per effetto di una falsa dichiarazione negligente è limitato alle perdite effettive. Ibidem § 552B (1).

In un caso recente, ad esempio, la Corte Superiore del Connecticut ha ritenuto che il fatto che un fornitore di energia elettrica avesse omesso di dichiarare di aver comunicato informazioni relative ai pagamenti dei clienti ad agenzie di credito nazionali giusitificava un'azione legale per falsa dichiarazione. Cfr. Brouillard v. United Illuminating Co., 1999 Conn. Super. LEXIS 1754. In quel caso, al ricorrente è stato rifiutato un credito perché il convenuto aveva riferito di pagamenti «tardivi» perché non ricevuti entro trenta giorni della data di fatturazione. Il ricorrente ha sostenuto di non essere stato informato di queste condizioni al momento dell'apertura del conto per la fornitura di elettricità. Il tribunale ha ritenuto che «l'omissione di una dichiarazione a cui il convenuto è obbligato può giustificare una denuncia per falsa dichiarazione negligente». Questo caso dimostra inoltre che la «intenzionalità» o l'intenzione fraudolenta non è un elemento necessario in un'azione legale per falsa dichiarazione negligente. Pertanto, un'organizzazione statunitense che per negligenza ometta di dichiarare in modo completo come utilizzerà le informazioni personali ricevute in base ai principi «approdo sicuro», potrebbe essere ritenuta responsabile di falsa dichiarazione.

In quanto comporta un uso improprio di dati personali, una violazione dei principi «approdo sicuro» potrebbe anche giustificare una denuncia della persona interessata per il reato di violazione delle privacy secondo la common law. La legge degli Stati Uniti riconosce da molto tempo cause di azione relative alla violazione della privacy. In una causa del 1905 (3), la Corte suprema della Georgia ha riconosciuto che il diritto alla privacy è radicato nel diritto naturale e nei precetti della common law nel giudicare il caso di un privato cittadino la cui fotografia era stata utilizzata da una compagnia di assicurazioni sulla vita senza il suo consenso o a sua insaputa per illustrare un annuncio pubblicitario. Formulando argomentazioni oggi familiari nella giurisprudenza americana relativa alla privacy, la corte ha dichiarato che l'uso della fotografia era «doloso», «falso» e tendente a «mettere in ridicolo il ricorrente di fronte a tutti» (4). Le motivazioni della sentenza Pavesich sono divenute, con minime variazioni, la base del diritto statunitense in materia. I tribunali degli Stati hanno costantemente sostenuto le cause d'azione nell'ambito della violazione della privacy e almeno 48 Stati riconoscono ora giudizialmente tali cause d'azione (5). Inoltre, in almeno dodici Stati esistono norme costituzionali che tutelano il diritto dei cittadini alla non intrusione (6), e che in alcuni casi potrebbero essere estese alla protezione da intrusioni commesse da organismi non governativi. Cfr. ad esempio Hill v. NCAA, 865 P.2d 633 (Ca. 1994); cfr. anche S. Ginder, Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet, 34 S.D. L. Rev. 1153 (1997) («Le costituzioni di alcuni Stati prevedono una tutela della privacy più rigorosa rispetto a quella della costituzione degli Stati Uniti, Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, Carolina del Sud e Washington sono gli Stati che assicurano una maggiore tutela della privacy»).

Il Second Restatement of Torts contiene un'autorevole rassegna della legge in questo campo. Rispecchiando la prassi giudiziaria comune, il Restatement spiega che il «diritto alla privacy» comprende quattro distinte cause di azione per illecito civile (cfr. Restatement, § 652A). In primo luogo, una causa d'azione per «intrusione nella sfera riservata» (intrusion upon seclusion) è ammissibile contro chi violi intenzionalmente, fisicamente o in altro modo, la solitudine o l'isola-

---

(3) Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).

(4) Ibidem, a 69.

(5) Una ricerca elettronica effettuata nella base di dati Westlaw ha rilevato 2 703 casi di azioni civili nei tribunali nazionali relativi alla «privacy» a partire dal 1995. Abbiamo già presentato alla Commissione i risultati di tale ricerca.

(6) Cfr. ad esempio Alaska Constitution, Art. 1, Sez. 22; Arizona, Art. 2, Sez. 8; California, Art. 1, Sez. 1; Florida, Art. 1, Sez. 23; Hawaii, Art. 1, Sez. 5; Illinois, Art. 1, Sez. 6; Louisiana, Art. 1, Sez. 5; Montana, Art. 2, Sez. 10; New York, Art. 1, Sez. 12; Pennsylvania, Art. 1, Sez. 1; South Carolina, Art. 1, Sez. 10; e Washington, Art. 1, Sez. 7.

mento di un altro o i suoi affari o interessi privati (7). In secondo luogo, una causa per «appropriazione» è giustificata qualora una persona assuma il nome o le sembianze di un'altra a suo uso o beneficio (8). In terzo luogo, la «pubblicità data a fatti privati» dà il diritto di proporre un'azione in giudizio quando l'evento reso pubblico è di natura tale da essere altamente offensivo per una persona ragionevole e non è di legittimo interesse pubblico (9). Infine, un'azione per «pubblicità calunniosa» è legittima quando il convenuto intenzionalmente o imprudentemente mette pubblicamente un'altra persona in cattiva luce in un modo altamente offensivo per qualsiasi persona ragionevole (10).

Nell'ambito dei principi «approdo sicuro», la «intrusione nella sfera riservata» potrebbe includere la raccolta non autorizzata di informazioni personali, mentre l'uso non autorizzato di dati personali a scopi commerciali potrebbe dar origine a una causa per «appropriazione». Analogamente, una divulgazione di dati personali che fosse inesatta potrebbe dare origine a un illecito civile per «pubblicità calunniosa» qualora le informazioni in questione abbiano la caratteristica di essere altamente offensive per una persona ragionevole. Infine, la violazione della privacy derivante dalla pubblicazione o divulgazione di dati personali sensibili potrebbe dar origine a una causa per «pubblicità data a fatti privati» (cfr. gli esempi riportati qui di seguito).

Per quanto concerne il risarcimento dei danni, le violazioni della privacy conferiscono alla parte lesa il diritto di ottenere un indennizzo per:

a) il pregiudizio per la privacy derivante dalla violazione;

b) il danno psicologico dimostrato, nel caso in cui esso sia di natura normalmente attribuibile ad una tale violazione;

c) ogni danno particolare di cui la violazione sia una causa legale.

Restatement, § 652H. Data l'applicabilità generale del diritto civile e la molteplicità delle cause d'azione riguardanti i diversi aspetti degli interessi connessi alla privacy, il risarcimento dei danni può essere richiesto da quanti hanno subito una violazione della privacy in conseguenza di un mancato rispetto dei principi «approdo sicuro».

I tribunali degli Stati sono sommersi da cause relative alla violazione della privacy in situazioni analoghe. Ex Parte AmSouth Bancorporation et al., 717 So. 2d 357, ad esempio, riguardava un'azione intentata da un gruppo di persone (class action) in cui il convenuto era accusato di «avere sfruttato la fiducia riposta nella banca dai depositanti, comunicando informazioni riservate sui depositanti ed i loro conti» per consentire a una banca affiliata di vendere fondi comuni di investimento ed altri tipi di investimenti. I danni vengono spesso risarciti in tali casi. Nella causa Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580 (D.C.App. 1985), una corte d'appello ha riformato la sentenza del tribunale di grado inferiore sostenendo che l'utilizzo delle fotografie del ricorrente «prima» e «dopo» un intervento di chirurgia plastica durante una presentazione in un grande magazzino costituiva una violazione della privacy attraverso la pubblicità data a fatti privati. In Candebat v. Flanagan, 487 So.2d 207 (Miss. 1986), la compagnia di assicurazioni convenuta aveva utilizzato un incidente in cui la moglie del ricorrente era rimasta gravemente ferita per una campagna pubblicitaria. Il ricorrente l'ha citata in giudizio per violazione della privacy. Il tribunale ha decretato il risarcimento dei danni subiti dal ricorrente per lo stress emotivo e l'appropriazione di identità. Le azioni legali per appropriazione indebita possono essere sostenute anche se il querelante non è un personaggio famoso. Cfr., ad esempio, Staruski v. Continental Telephone Co., 154 Vt. 568 (1990) (il convenuto ha ottenuto vantaggi commerciali utilizzando il nome e la fotografia di un dipendente in un'inserzione pubblicitaria). In Pulla v. Amoco Oil Co., 882 F.Supp. 836 (S.D Iowa 1995), un datore di lavoro ha violato la riservatezza del dipendente ricorrente chiedendo ad un altro dipendente di effettuare controlli sui movimenti della sua carta di credito per verificare i giorni di assenza per malattia. Il tribunale ha concesso un risarcimento di 2 USD a titolo di indennizzo per danni reali e di 500 000 USD come sanzione. Un altro datore di lavoro è stato ritenuto responsabile per aver pubblicato un articolo nel giornale dell'azienda riguardante un dipendente che era stato licenziato per aver falsificato le timbrature del suo cartellino. Cfr. Zinda v. Louisiana-Pacific Corp., 140 Wis.2d 277 (Wis. App. 1987). L'articolo aveva violato la privacy del ricorrente rendendo pubblico un fatto privato tramite un giornale diffuso nella comunità. Infine, un college che aveva sottoposto i suoi studenti al test dell'HIV dopo aver detto loro che il prelievo di sangue sarebbe servito solo per un test sulla rosolia è stato giudicato responsabile di intrusione nella sfera riservata. Cfr. Doe v. High-Tech Institute, Inc., 972 P.2d 1060 (Colo. App. 1998). (Per altri casi menzionati, cfr. Restatement, § 652H, Appendix.)

Gli Stati Uniti sono spesso criticati per il ricorso eccessivo ad azioni giudiziarie, ma ciò significa anche che i singoli possono effettivamente adire le vie legali qualora ritengano di essere stati danneggiati. Molti aspetti del sistema giudiziario

(7) Ibidem, Capitolo 28, Sezione 652B.
(8) Ibidem, Capitolo 28, Sezione 652C.
(9) Ibidem, Capitolo 28, Sezione 652D.
(10) Ibidem, Capitolo 28, Sezione 652E.

americano rendono più facile per chi subisce un torto intentare un'azione, sia individualmente, sia come categoria. L'avvocatura, comparativamente più ampia che nella maggior parte degli altri paesi, rende la rappresentanza professionale immediatamente disponibile. L'avvocato di parte civile, che rappresenta i singoli nelle cause private, decide liberamente i propri onorari e questo permette anche a persone con basso reddito di chiedere un risarcimento danni. Questo è un aspetto importante: negli Stati Uniti ciascuna parte paga abitualmente gli onorari dei propri avvocati e le altre spese legali, contrariamente alla prassi prevalente in Europa, dove la parte soccombente deve rimborsare all'altra parte le spese processuali sostenute. Senza dibattere dei vantaggi dei due sistemi, è meno probabile che la prassi americana dissuada dall'intentare una causa legittima le persone che non sarebbero in grado di sostenere le spese di entrambe le parti se dovessero perdere la causa.

I singoli possono chiedere il risarcimento dei danni anche per somme relativamente esigue. Nella maggior parte delle giurisdizioni americane, se non in tutte, esistono tribunali per le cause di modesta entità (small claims courts) che garantiscono procedure semplificate e meno costose per le controversie di valore inferiore al limite fissato dalla legge ([11]). Anche le possibili sanzioni pecuniarie (punitive damages) offrono una compensazione finanziaria alle persone che hanno subito un lieve danno diretto e che fanno causa per una condotta scorretta riprovevole. Infine, le persone che hanno subito un danno identico possono mettere in comune le loro risorse e la loro azione in giudizio per intentare una causa in quanto categoria o gruppo (class action).

Un ottimo esempio di come i singoli possano intentare una causa per ottenere il risarcimento di danni è la causa in corso contro Amazon.com per violazione della privacy. Amazon.com, il grande sito di commercio elettronico, è oggetto di un'azione legale da parte di un gruppo di persone che sostengono di non essere stati informati e di non aver dato il loro consenso alla raccolta di dati personali quando hanno utilizzato il software «Alexa» di proprietà di Amazon. In questa causa gli attori hanno invocato una violazione del Computer Fraud and Abuse Act per l'accesso illecito alle comunicazioni memorizzate e dell'Electronic Communications Privacy Act per l'intercettazione illegale delle loro comunicazioni elettroniche e telefoniche. Essi denunciano anche una violazione delle privacy secondo l'accezione della common law. All'origine, vi è una denuncia presentata da un esperto in sicurezza su Internet nel mese di dicembre. La richiesta di risarcimento è di 1 000 USD per ognuna delle persone del gruppo, più l'onorario degli avvocati e il rimborso dei guadagni resi possibili dalla violazione delle leggi. Poiché il numero di queste persone dovrebbe essere dell'ordine di milioni, il risarcimento danni totale potrebbe ammontare a miliardi di dollari. Anche la FTC (Federal Trade Commission) sta esaminando i capi d'imputazione.

*La legislazione federale e la legislazione degli Stati sulla privacy prevedono spesso cause d'azione private per il risarcimento pecuniario.*

Oltre a dar origine alla responsabilità civile nell'ambito del diritto degli atti illeciti (tort law), l'inosservanza dei principi «approdo sicuro» può anche comportare la violazione di qualcuna delle centinaia di leggi federali e dei singoli Stati sulla privacy. Molte di queste leggi concernenti il trattamento dei dati personali nei settori pubblico e privato consentono ai singoli di chiedere il risarcimento dei danni qualora si verifichi una violazione. Ad esempio:

Electronic Communications Privacy Act del 1986. L'ECPA vieta l'intercettazione non autorizzata delle chiamate telefoniche tramite cellulare e delle trasmissioni da computer a computer. Le violazioni possono comportare una responsabilità civile non inferiore a 100 USD per ogni giorno di violazione. La tutela dell'ECPA si estende anche all'accesso non autorizzato o alla divulgazione delle comunicazioni elettroniche memorizzate. I trasgressori sono responsabili dei danni subiti o dei mancati guadagni per effetto di una violazione.

Telecommunications Act del 1996. A norma della sezione 702, le informazioni sulla rete di proprietà riservata dell'utente (CPNI) non possono essere utilizzate per uno scopo diverso dalla fornitura di serivizi di telecomunicazione. Gli abbonati al servizio possono o presentare una denuncia alla Federal Communications Commission o presentare istanza di risarcimento dei danni e di rimborso degli onorari degli avvocati presso il tribunale del distretto federale.

Consumer Credit Reporting Reform Act del 1996. La legge del 1996 ha emendato il Fair Credit Reporting Act del 1970 (FCRA) per richiedere un'ulteriore notifica e diritto di accesso per i soggetti di informazioni commerciali. Il Reform Act ha anche imposto nuove restrizioni sui rivenditori di informazioni commerciali sui consumatori. I consumatori possono ottenere il risarcimento dei danni e il rimborso degli onorari degli avvocati in caso di violazione.

([11]) Abbiamo già fornito alla Commissione le informazioni relative alle azioni di modesta entità.

Le leggi degli Stati tutelano anche la sfera privata delle persone in un'ampia gamma di situazioni. Gli Stati hanno adottato provvedimenti che riguardano i rendiconti bancari, gli abbonamenti alle televisioni via cavo, le informazioni commerciali, gli stati di servizio, la documentazione amministrativa, le informazioni genetiche e le cartelle cliniche, le polizze assicurative, le pagelle, le comunicazioni elettroniche ed il noleggio di videocassette [12].

B. **Autorizzazioni legali esplicite**

I principi «approdo sicuro» contengono un'eccezione qualora atti legislativi, regolamenti o la giurisprudenza «comportino obblighi contrastanti od autorizzazioni esplicite, purché nell'avvalersi di un'autorizzazione siffatta un'organizzazione possa dimostrare che il mancato rispetto dei principi da parte sua si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione». È ovvio che quando la legge statunitense impone un'obbligazione conflittuale, le organizzazioni statunitensi, che aderiscano o no ai principi «approdo sicuro», devono osservare la legge. Per quanto riguarda le autorizzazioni esplicite, sebbene i principi «approdo sicuro» intendano colmare le differenze tra il sistema americano e quello europeo relativamente alla tutela della privacy, siamo tenuti al rispetto delle prerogative legislative dei legislatori eletti. La limitata eccezione al rigoroso rispetto dei principi «approdo sicuro» cerca di stabilire un equilibrio in grado di conciliare i legittimi interessi delle parti.

L'eccezione è limitata ai casi in cui esiste un'autorizzazione esplicita. Tuttavia, come caso limite, la legge, il regolamento o la decisione del tribunale pertinenti devono esplicitamente autorizzare una particolare condotta delle organizzazioni aderenti ai principi «approdo sicuro» [13]. In altre parole, l'eccezione non verrà applicata se la legge non prescrive nulla. Inoltre, l'eccezione verrà applicata soltanto se l'esplicita autorizzazione è in conflitto con il rispetto dei principi «approdo sicuro». Anche in questo caso, l'eccezione «si limita a quanto strettamente necessario per soddisfare i legittimi interessi d'ordine superiore tutelati da detta autorizzazione». Ad esempio, se la legge si limita ad autorizzare un'azienda a fornire dati personali alle pubbliche autorità, l'eccezione non verrà applicata. Al contrario, se la legge autorizza espressamente l'azienda a fornire dati personali ad organizzazioni governativi senza il consenso dei singoli, ciò costituisce una «autorizzazione esplicita» ad agire in contrasto con i principi «approdo sicuro». In alternativa, le specifiche eccezioni alle disposizioni relative alla notifica al consenso rientrerebbero nell'ambito dell'eccezione (dato che ciò equivarrebbe ad una specifica autorizzazione a rivelare informazioni senza notifica e consenso). Ad esempio, una legge che autorizzi i medici a fornire le cartelle cliniche dei loro pazienti agli ufficiali sanitari senza il previo consenso dei pazienti stessi potrebbe consentire un'eccezione ai principi di notifica e di scelta. Tale autorizzazione non permetterebbe ad un medico di fornire le stesse cartelle cliniche alle casse mutue malattie o ai laboratori di ricerca farmaceutica perché ciò esulerebbe dall'ambito degli usi consentiti dalla legge e dunque dall'ambito dell'eccezione [14]. L'autorizzazione in questione può essere un'autorizzazione «autonoma» a fare determinate cose con i dati personali ma, come illustrato negli esempi di cui sopra, è probabile che si tratti di un'eccezione a una legge generale che proscrive la raccolta, l'uso o la divulgazione dei dati personali.

*Telecommunications Act del 1996*

In molti casi, gli usi autorizzati sono conformi alle disposizioni della direttiva e ai principi oppure sono consentiti dall'una o dall'altra delle eccezioni ammesse. Ad esempio, la sezione 702 del Telecommunications Act (codificato in 47 U.S.C. § 222) impone agli operatori delle telecomunicazioni l'obbligo di mantenere riservati i dati personali ottenuti nel corso della fornitura dei loro servizi agli utenti. Tale disposizione consente in particolare agli operatori delle telecomunciazioni di:

1. utilizzare le informazioni relative agli utenti per offrire un servizio di telecomunicazione, inclusa la pubblicazione dei numeri di telefono degli abbonati;

2. fornire informazioni sugli utenti a terzi dietro richiesta scritta dell'utente; e

3. fornire informazioni sugli utenti in forma aggregata.

(12) Una recente ricerca elettronica sulla base di dati Westlaw ha individuato 994 cause per risarcimento danni e violazione della privacy.

(13) Come elemento di chiarificazione, l'autorizzazione legale pertinente non dovrà far specifico riferimento ai principi «approdo sicuro».

(14) Analogamente, il medico dell'esempio non potrebbe basarsi su un'autorizzazione legale per non tenere conto della possibilità di rifiutare la commercializzazione diretta prevista per i singoli dalla FAQ 12. L'ambito di qualsiasi eccezione per «autorizzazione esplicita» è necessariamente limitato all'ambito dell'autorizzazione conformemente alla legge in materia.

Cfr. 47 U.S.C. § 222(c)(1)-(3). La legge ammette anche un'eccezione nell'utilizzo delle informazioni relative agli utenti da parte degli operatori delle telecomunicazioni:

1. per l'avvio, la prestazione, la fatturazione e la riscossione per i servizi resi;

2. per la protezione contro i comportamenti fraudolenti, abusivi o illegali;

3. per la fornitura di servizi di telemarketing, assistenza o amministrativi nel corso di una chiamata da parte dell'utente ([15]).

Ibidem, § 222(d)(1)-(3). Infine, gli operatori delle telecomunicazioni sono tenuti a fornire agli editori degli elenchi telefonici informazioni sull'elenco degli abbonati che includano soltanto il nome, l'indirizzo, il numero di telefono e il settore d'attività per gli utenti commerciali. Ibidem, § 222(e).

L'eccezione per «autorizzazioni esplicite» potrebbe entrare in gioco qualora gli operatori delle telecomunicazioni utilizzino CPNI per prevenire la frode o altri comportamenti illegali. Anche in questo caso, tali azioni potrebbero essere considerate di «interesse pubblico» e consentite per questa ragione dai principi.

*Norme proposte dal ministero della Sanità*

Il ministero della Sanità (HHS) ha proposto alcune norme riguardanti gli standard della privacy relativamente alle informazioni sanitarie individualmente identificabili. Cfr. 64 Fed. Reg. 59,918 (3 novembre 1999) (da codificare in 45 C.F.R. pts. 160–164). Tali norme daranno attuazione alle disposizioni sulla privacy del Health Insurance Portability and Accountability Act del 1996. Pub. L. 104–191. Le norme proposte vieterebbero in linea generale alle entità interessate (quali sistemi sanitari, stanze di compensazione sanitarie ed operatori sanitari che trasmettono informazioni sanitarie in formato elettronico) l'utilizzo o la divulgazione di informazioni sanitarie riservate senza l'autorizzazione dei singoli. Cfr. proposta 45 C.F.R. § 164.506. Le norme proposte consentiranno la divulgazione di informazioni sanitarie protette soltanto per due motivi: 1) per consentire ai singoli di esaminare e copiare le informazioni sanitarie sul proprio conto, cfr. ibidem § 164.514; e 2) per far rispettare le regole, cfr. ibidem § 164.522.

Le norme proposte consentirebbero l'uso o la divulgazione di informazioni sanitarie protette, senza la specifica autorizzazione dei singoli, in limitate circostanze. Queste ultime includono ad esempio la supervisione del sistema sanitario, l'applicazione della legge, e le emergenze. Cfr. al § 164.510. Le norme proposte fissano nei dettagli i limiti di tali usi o divulgazioni. Inoltre, gli usi consentiti e le divulgazioni delle informazioni sanitarie protette sarebbero limitati alla quantità minima necessaria. Cfr. ibidem al § 164.506.

Gli usi esplicitamente autorizzati dalle disposizioni proposte sono generalmente conformi ai principi «approdo sicuro» o sono altrimenti consentiti da un'altra eccezione. Ad esempio, l'applicazione della legge e l'amministrazione giudiziaria sono consentiti, come pure la ricerca medica. Altri usi, quali la supervisione del sistema sanitario, la funzione della salute pubblica ed i sistemi informativi sanitari nazionali sono di pubblico interesse. Le divulgazioni che servono per esaminare le richieste di contributi ed esenzioni sanitarie sono necessarie per garantire l'assistenza sanitaria. Gli usi in situazioni di emergenza, per la consultazione in caso di un parente prossimo riguardo a un trattamento quando il consenso del paziente «non può praticamente o ragionevolmente essere ottenuto» o per determinare la natura o la causa della morte del deceduto, proteggono gli interessi vitali del soggetto e degli altri. Gli usi per la gestione dei militari in servizio effettivo ed altre particolari categorie di persone facilita l'appropriata esecuzione della missione militare o di simili situazioni urgenti; in ogni caso, tali usi avranno una ripercussione limitata o nulla sui consumatori in generale.

È consentito soltanto l'utilizzo di informazioni personali da parte delle strutture sanitarie per la pubblicazione degli elenchi nominativi dei pazienti. Anche se un tale uso potrebbe non raggiungere il livello di un interesse «vitale», tali

([15]) L'ambito di tale eccezione è molto limitato. In quanto tale, l'operatore delle telecomunicazioni può utilizzare CPNI soltanto durante una chiamata fatta dal cliente. Inoltre, siamo stati informati dalla FCC che esso non può utilizzare CPNI per commercializzare servizi che esulino dall'ambito della richiesta dell'utente. Infine, dato che l'utente deve approvare l'uso di CPNI a tale scopo, questa disposizione non costituisce realmente una «eccezione».

elenchi costituiscono un vantaggio reale per i pazienti, i loro amici e parenti. Anche l'ambito di tale uso autorizzato è intrinsecamente limitato. Pertanto, il ricorso all'eccezione ai principi per gli usi «esplicitamente autorizzati» dalla legge a tale scopo presenta un rischio minimo per la privacy dei pazienti.

*Fair Credit Reporting Act*

La Commissione europea ha espresso preoccupazioni per il fatto che l'eccezione per «autorizzazioni esplicite» possa «dar luogo efficacemente a un accertamento di adeguatezza» relativamente al Fair Credit Reporting Act (FCRA). Questo non è il caso. In mancanza di uno specifico giudizio di adeguatezza relativo al FCRA, le società americane che altrimenti si baserebbero su tale giudizio dovrebbero impegnarsi ad attenersi sotto tutti gli aspetti ai principi «approdo sicuro». Ciò significa che, qualora le disposizioni del FCRA superino il livello di protezione assicurato dai principi, le organizzazioni americane devono soltanto rispettare il FCRA. Nel caso in cui, invece, il FCRA fosse insufficiente, tali organizzazioni dovranno conformare ai principi le loro prassi in materia d'informazione. L'eccezione non modifica la valutazione di base. Per sua natura, l'eccezione è applicabile soltanto quando la legge pertinente autorizza esplicitamente un comportamento che non sarebbe conforme ai principi «approdo sicuro». L'eccezione non verrebbe applicata nel caso in cui le disposizione del FCRA non corrispondono ai principi «approdo sicuro» ([16]).

In altre parole, non intendiamo l'eccezione nel senso che ciò che non è obbligatorio è «esplicitamente autorizzato». Inoltre, l'eccezione è applicabile soltanto quando ciò che è esplicitamente autorizzato dalla legge degli Stati Uniti è in conflitto con le disposizione dei principi «approdo sicuro». La legge in questione deve soddisfare entrambi questi elementi prima che sia autorizzata la non conformità ai principi.

La sezione 604 del FCRA, ad esempio, autorizza esplicitamente le consumer reporting agencies a pubblicare informazioni sui consumatori nelle varie situazioni specificate. Cfr. FCRA, § 604. Se in tal modo la sezione 604 autorizza le agenzie ad operare in contrasto con i principi «approdo sicuro», esse devono ricorrere all'eccezione (a meno che, naturalmente, non sia applicabile un'altra eccezione). Le credit reporting agencies devono conformarsi alle ordinanze del tribunale e alle ingiunzioni del grand jury e l'uso delle informazioni da parte delle agenzie autorizzate, degli enti sociali e di sostegno all'infanzia ha una finalità pubblica. Ibidem, § 604(a)(1), (3)(D), e (4). Di conseguenza, la credit reporting agency non avrebbe bisogno di far ricorso per questi scopi all'eccezione della «autorizzazione esplicita». Se agisce conformemente alle istruzioni scritte dell'utente, l'agenzia si conforma pienamente ai principi «approdo sicuro». Ibidem, § 604(a)(2). Similmente, le informazioni sui consumatori possono essere ottenute per scopi attinenti all'occupazione soltanto con il conseno scritto dei consumatori stessi [ibidem, §§ 604(a)(3)(B) e (b)(2)(A)(ii)] e per le operazioni creditizie o assicurative che non sono di iniziativa del consumatore soltanto se questi non ha scelto di esserne escluso [ibidem, § 604(c)(1)(B)]. Il FCRA vieta anche alle credit reporting agencies di fornire informazioni sanitarie per scopi attinenti all'occupazione senza il consenso del consumatore. Ibidem, § 604(g). Questi usi sono conformi ai principi di notifica e di scelta. Le altre finalità autorizzate dalla sezione 604 riguardano le transazioni che implicano il consumatore e sono per tale motivo consentite dai principi. Cfr. ibidem, § 604(a)(3)(A) e (F).

L'ultimo uso «autorizzato» dalla sezione 604 riguarda i mercati secondari del credito. Ibidem, § 604(a)(3)(E). Non c'è di per sé conflitto tra l'uso di informazioni sui consumatori e i principi «approdo sicuro». È vero che il FCRA non prevede, ad esempio, che le credit reporting agencies notifichino ai consumatori o chiedano il loro consenso all'atto della pubblicazione di informazioni a tale scopo. Tuttavia, ribadiamo che l'assenza di un obbligo non implica una «autorizzazione esplicita» ad agire in un modo diverso da quello prescritto. Analogamente, la sezione 608 consente alle credit reporting agencies di fornire dati personali a organismi pubblici. Una tale «autorizzazione» non giustifica che una credit reporting agency ignori il suo impegno a rispettare i principi «approdo sicuro». Ciò contrasta con gli altri nostri esempi in cui le eccezioni ai principi di notifica affermativa e di scelta servono ad autorizzare esplicitamente l'uso di dati personali senza notifica o scelta.

*Conclusione*

Dalla nostra sommaria rassegna di queste leggi emergono distintamente alcune linee:

— «L'autorizzazione esplicita» consente generalmente l'uso o la divulgazione di dati personali senza il previo consenso del singolo; perciò, l'eccezione è limitata ai principi di notifica e di scelta.

([16]) Queste nostre osservazioni non vanno intese come un'ammissione del fatto che il FCRA non prevede una «adeguata» protezione. Una valutazione del FCRA deve tener conto della tutela assicurata dalla legge nella sua interezza e non concentrarsi sulle sole eccezioni, come facciamo qui.

— Nella maggior parte dei casi, le eccezioni autorizzate dalla legge sono definite in modo preciso per essere applicate in situazioni e per finalità specifiche. In tutti i casi la legge vieta altrimenti l'uso non autorizzato o la divulgazione di dati personali al di fuori di questi limiti.

— Nella maggior parte dei casi, rispecchiando la loro natura legislativa, l'uso o la divulgazione autorizzata sono di pubblico interesse.

— In quasi tutti i casi, gli usi autorizzati sono o pienamente conformi ai principi «approdo sicuro» o rientrano in una delle altre eccezioni ammesse.

In conclusione, l'eccezione per «esplicite autorizzazioni» prevista dalla legge avrà probabilmente, per sua natura, un campo d'applicazione alquanto limitato.

C. **Fusioni e acquisizioni**

Il gruppo di lavoro «articolo 29» ha espresso preoccupazione per le situazioni in cui un'organizzazione che ha aderito ai principi «approdo sicuro» viene rilevata da o si fonde con una società che non ha assunto l'impegno di rispettare tali principi. Il gruppo di lavoro sembra ritenere che l'azienda rilevante non sia tenuta ad applicare i principi «approdo sicuro» ai dati personali in possesso dell'azienda rilevata, ma questo non è necessariamente il caso per la legge degli Stati Uniti. La regola generale negli Stati Uniti per quanto concerne le fusioni e le acquisizioni è che la società che acquista il capitale sociale di un'altra si assume generalmente gli obblighi e le resonsabilità della società rilevata. Cfr. 15 Fletcher Cyclopedia of the Law of Private Corporations § 7117 (1990); cfr. anche Model Bus. Corp. Act § 11.06(3) (1979) («la società risultante assume tutte le responsabilità delle società partecipanti alla fusione»). In altre parole, la società che rileva per fusione o acquisizione un'impresa che ha aderito ai principi «approdo sicuro» sarà in questo modo vincolata dagli impegni assunti da quest'ultima.

Inoltre, anche se la fusione o l'acquisizione fossero effettuate tramite il trasferimento di attivi, le responsabilità della società acquisita vincolerebbero comunque la società acquisente in alcune circostanze. 15 Fletcher, § 7122. Anche nel caso in cui le responsabilità non sopravvivessero alla fusione, va tuttavia osservato che queste non sopravviverebbero ad una fusione qualora i dati fossero trasferiti dall'Europa in base ad un contratto (la sola alternativa possibile all'approdo sicuro per il trasferimento di dati negli Stati Uniti). Inoltre, i documenti «approdo sicuro» nella loro versione modificata richiedono ora che ogni impresa che abbia aderito ai principi notifichi al Dipartimento del commercio ogni acquisizione e permettono che i dati continuino ad essere trasferiti alla società subentrante solo se essa aderisce ai principi (cfr. FAQ 6). In virtù delle modifiche ora apportate al quadro «approdo sicuro», le società americane che si trovano in questa situazione hanno l'obbligo di cancellare le informazioni ricevute in tale quadro nel caso in cui gli impegni da loro assunti non siano mantenuti o non siano adottate altre salvaguardie adeguate.

———

*ALLEGATO V*

14 luglio 2000

John Mogg
Direttore, DG XV
Commissione europea
Ufficio C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Bruxelles

Egregio sig. Mogg,

Vedo che la mia lettera del 29 marzo 2000 ha suscitato varie questioni. Per precisare le competenze della Commissione federale del commercio (FTC) nei campi in relazioni ai quali sono sorte questioni, Le invio la presente che, per facilitare i nostri futuri scambi di vedute, completa e riassume il contenuto di parte della precedente corrispondenza.

Nelle Sue visite ai nostri uffici e nella Sua corrispondenza, Lei ha posto varie domande sull'autorità della Commissione federale del commercio degli Stati Uniti in materia di protezione della sfera privata «online». Ho pensato che sarebbe stato utile riassumere le mie risposte precedenti e fornirLe maggiori ragguagli sulla competenza della FTC per quanto riguarda i problemi di tutela della sfera privata del consumatore da Lei sollevati nella Sua ultima lettera. Più in particolare, Lei chiede 1) se la FTC è competente per i trasferimenti di dati relativi all'occupazione effettuati in violazione dei principi statunitensi «approdo sicuro»; 2) se la FTC è competente per i sistemi di omologazione («seal») senza scopo di lucro; 3) se il FTC Act si applica tanto ai dati «offline» quanto a quelli «online»; che cosa accade quando la giurisdizione della FTC si sovrappone a quella di altri organi preposti all'applicazione della legge.

*Applicazione del FTC Act alla tutela della sfera privata*

In questo settore, la competenza della Commissione federale del commercio è definita alla sezione 5 del Federal Trade Commission Act («FTC Act»), che proibisce «atti o pratiche sleali o fraudolente» [1]. Per pratica fraudolenta s'intende una rappresentazione, un'omissione o una pratica che possa indurre materialmente in errore i normali consumatori. Una pratica è considerata sleale se causa — o può causare — ai consumatori un danno grave che non può essere ragionevolmente evitato e che non è compensato da vantaggi per i consumatori o per la concorrenza [2].

Alcuni metodi di raccolta dei dati possono comportare una violazione del FTC Act. Ad esempio, se un sito Internet dichiara falsamente di attenersi a una politica di tutela della sfera privata o una serie di principi d'autoregolamentazione, la sezione 5 del FTC Act costituisce una base giuridica che permette di contestare il carattere fraudolento di questa dichiarazione falsa. Infatti, l'applicazione efficace della legge ci ha permesso di stabilire questo principio [3]. In base alla posizione che ha adottato, inoltre, la FTC può contestare come sleali pratiche di particolare gravità per quanto riguarda la tutela della sfera privata quando tali pratiche concernono bambini o l'utilizzo di informazioni di natura molto sensibile, ad esempio di carattere finanziario [4] o medico. La Commissione federale del commercio continuerà ad adoperarsi per garantire l'applicazione della legge svolgendo un'azione di sorveglianza e di indagine, e grazie alle denunce presentate da organizzazioni d'autoregolamentazione e da altri, compresi gli Stati membri dell'Unione europea.

---

[1] 15 U.S.C. § 45. Il Fair Credit Reporting Act si applicherebbe anche alla raccolta e alla vendita di dati Internet che corrispondono alle definizioni legali di «consumer report» e di «consumer reporting agency».

[2] 15 U.S.C. § 45(n).

[3] Cfr. GeoCities, Docket No. C-3849 (Final Order del 12 febbraio 1999) (cf.: www.ftc.gov/os/1999/9902/9823015d%26o.htm); Liberty Financial Cos., Docket nº C-3891 (Final Order del 12 agosto 1999) (cf.: www.ftc.gov/opa/1999/9905/younginvestor.htm). Cfr. anche Children's Online Privacy Protection Act Rule (COPPA), 16 C.F.R. Parte 312 (cf.: www.ftc.gov/opa/1999/9910/childfinal.htm). Il regolamento COPPA, che è entrato in vigore il mese scorso, prevede che gli operatori di siti Internet che si rivolgono a bambini di meno di 13 anni o che raccolgono deliberatamente dati a carattere personale da bambini di meno di 13 anni, debbano applicare i principi del codice di deontologia dell'informazione enunciati nel regolamento.

[4] Cfr. FTC v. Touch Tone, Inc., Civil Action No 99-WM-783 (D.Co.) (registrata il 21 aprile 1999), cf. www.ftc.gov/opa/1999/9904/touchtone.htm. Parere del personale del 17 luglio 1997, in risposta ad una petizione depositata dal Center for Media Education, cf. www.ftc.gov/os/1997/9707/cenmed.htm.

*Sostegno all'autoregolamentazione*

La FTC darà la precedenza alle denunce d'inosservanza dei principi d'autoregolamentazione pervenute da organizzazioni come BBBOnline o TRUSTe ([5]).

Quest'approccio è coerente con le relazioni che manteniamo da tempo con il National Advertising Review Board (NARB) del Better Business Bureau, che trasmette alla FTC i reclami in materia di pubblicità. La National Advertising Division (NAD) del NARB tratta i reclami in materia di pubblicità a livello nazionale mediante una procedura arbitrale. Quando una parte rifiuta di conformarsi ad una decisione della NAD, la questione è deferita alla FTC. Il personale della FTC esamina, in via prioritaria, la pubblicità contestata per determinare se essa viola il FTC Act e spesso riesce a porre fine alla pratica contestata o a convincere la parte interessata ad attenersi al processo del NARB.

Analogamente, la FTC tratterà in via prioritaria i casi d'inosservanza dei principi «approdo sicuro» denunciati da Stati membri dell'UE. Come per le denunce che provengono da organizzazioni d'autoregolametazione statunitensi, il nostro personale terrà conto di tutte le informazioni che permettono di determinare se la pratica contestata viola la sezione 5 del FTC Act. Quest'impegno è anche espresso nei principi «approdo sicuro», FAQ 11 relativa all'applicazione delle decisioni.

*GeoCities: il primo caso di violazione della sfera privata su Internet sottoposto alla FTC*

GeoCities, il primo caso di violazione della sfera privata su Internet è stato sottoposto alla Commissione federale del commercio in virtù della sezione 5 ([6]). In questo caso, la FTC ha sostenuto che GeoCities presentava in modo ingannevole, tanto ai bambini che agli adulti, il modo in cui sarebbero stati utilizzati i loro dati di carattere personale. Secondo la denuncia alla FTC, GeoCities avrebbe dichiarato che alcuni dati di carattere personale raccolti nel suo sito Internet erano destinati solo ad un uso interno o per fornire ai consumatori offerte promozionali e prodotti o servizi da loro richiesti e che ulteriori dati «facoltativi» non sarebbero stati diffusi senza l'approvazione del consumatore. In realtà, queste informazioni sono state comunicate a terzi che li hanno utilizzati per indirizzare ai consumatori richieste oltre i limiti da essi accettati. GeoCities è anche accusato di ricorrere a pratiche fraudolente in relazione alla raccolta di informazioni presso i bambini. Secondo la denuncia, GeoCities asseriva di gestire uno spazio riservato ai bambini nel suo sito Internet e di conservare le informazioni ivi raccolte. In realtà, queste pagine erano gestite da terzi che raccoglievano e conservavano i dati.

La composizione della controversia vieta a GeoCities di fornire informazioni erronee circa lo scopo per il quale raccoglie o utilizza informazioni a carattere personale riguardanti i consumatori, compresi i bambini. La sentenza impone alla società di far figurare nel suo sito Internet un'avvertenza chiara e visibile sulla tutela della sfera privata, che indichi ai consumatori quali sono i dati raccolti e a quale scopo, a chi saranno comunicati e come essi possono accedere a questi dati ed eliminarli. Per garantire il controllo dei genitori, GeoCities deve ottenere il consenso dei genitori prima di raccogliere informazioni a carattere personale presso bambini di meno di 13 anni. GeoCities è tenuto ad informare i suoi membri e a dare loro la possibilità di fare cancellare dalle basi di dati di GeoCities e di terzi le informazioni che li riguardano. La sentenza prevede espressamente che GeoCities debba informare i genitori dei bambini di meno di 13 anni e cancellare le informazioni che li riguardano, a meno che i genitori diano il loro consenso esplicito alla loro conservazione e utilizzazione. Infine, GeoCities deve chiedere ai terzi a cui ha precedentemente comunicato informazioni di cancellare tali informazioni ([7]).

*ReverseAuction.com*

Nel gennaio 2000 la FTC ha accolto una denuncia presentata contro e un «consent agreement» con ReverseAuction.com, un sito di vendite all'asta che avrebbe ottenuto da un sito concorrente (eBay.com) informazioni a carattere personale sui consumatori e quindi inviato messaggi elettronici fraudolenti e non richiesti ai consumatori interessati dalle loro attività ([8]). Secondo la nostra denuncia, ReverseAuction aveva violato la sezione 5 del FTC Act ottenendo dati

---

([5]) La FTC ha presentato di recente una denuncia al tribunale distrettuale federale contro una società detentrice del marchio TRUSTe, Toysmart.com, per ottenere un'ingiunzione che impedisse la vendita di dati personali riservati raccolti sul sito web della società in violazione dei suoi principi in materia di privacy. La FTC è venuta a conoscenza di questa possibile violazione della legge direttamente da TRUSTe. FTC v. Toysmart.com, LLC, Civil Action No. 00-11341-RGS (D.Ma.) (11 luglio 2000) (disponibile in www.ftc.gov/opa/2000/07/toysmart.htm).

([6]) GeoCities, Docket No. C-3849 (Final Order del 12 febbraio 1999) (cf. www.ftc.gov/os/1999/9902/9823015d%26o.htm).

([7]) Successivamente, la FTC ha risolto un altro caso riguardante la raccolta su Internet di dati a carattere personale presso bambini. Liberty Financial Companies, Inc. gestiva il sito Internet Young Investor, indirizzato ai bambini e agli adolescenti e dedicato a questioni di denaro e d'investimenti. La FTC ha sostenuto che il sito dichiarava falsamente che i dati a carattere personale raccolti presso i bambini per mezzo di un'indagine sarebbero stati conservati in modo anonimo e che i partecipanti avrebbbero ricevuto un bollettino d'informazione elettronico e dei premi. In realtà, i dati personali riguardanti i bambini e la situazione finanziaria della famiglia erano conservati in modo identificabile e nessun bollettino né premio era stato inviato. L'accordo raggiunto proibisce queste presentazioni ingannevoli in futuro e impone a Liberty Financial di far figurare un'avvertenza sulla tutela della sfera privata nei suoi siti per bambini e di ottenere l'approvazione verificabile dei genitori prima di raccogliere dati a carattere personale presso i bambini. Liberty Financial Cos., Docket No. C-3891 (Final Order del 12 agosto 1999) (cf: www.ftc.gov/opa/1999/9905/younginvestor.htm).

([8]) Cfr. ReverseAuction.com, Inc., Civil Action No. 000032 (D.D.C.) (registrata il 6 gennaio 2000) (comunicato stampa e atti processuali in: www.ftc.gov/opa/2000/01/reverse4.htm).

di carattere personale, tra cui gli indirizzi elettronici e i codici d'identificazione personale degli utenti di eBay e inviando messaggi elettronici fraudolenti.

Come precisato nella denuncia, prima di ottenere queste informazioni ReverseAuction si è registrato come utente di eBay e ha accettato di aderire all'accordo sulla protezione della sfera privata degli utenti di questa società. Quest'accordo tutela la sfera privata dei consumatori vietando agli utenti di eBay di raccogliere e utilizzare dati a carattere personale a fini non autorizzati, come la spedizione di messaggi elettronici commerciali non richiesti. Di conseguenza, nella nostra denuncia si imputa in primo luogo a ReverseAuction di avere dichiarato falsamente che avrebbe rispettato l'accordo sulla tutela della sfera privata degli utenti di eBay, il che costituisce una pratica fraudolenta ai sensi della sezione 5. Inoltre, l'uso da parte di ReverseAuction di queste informazioni per inviare messaggi elettronici commerciali non richiesti, in violazione dell'accordo per la tutela della sfera privata degli utenti, costituisce una pratica commerciale sleale ai sensi della sezione 5.

In secondo luogo, abbiamo denunciato che i messaggi elettronici inviati ai consumatori contenevano una «linea oggetto» che poteva indurli in errore perché li informava che il loro codice d'identificazione eBay «sarebbe scaduto tra breve». Infine, nella denuncia si rileva che nei messaggi elettronici si affermava falsamente che eBay forniva a ReverseAuction, direttamente o indirettamente, dati a carattere personale sui suoi utenti o partecipava in altro modo alla diffusione di messaggi elettronici non richiesti.

La composizione della controversia ottenuta dalla FTC vieta a ReverseAuction di commettere in futuro simili infrazioni e gli impone di comunicare ai consumatori che si sono iscritti o desiderano iscriversi a ReverseAuction dopo aver ricevuto un suo messaggio di posta elettronica che il loro codice d'identificazione presso eBay non era in procinto di scadere e che eBay non era stato informato dell'invio da parte di ReverseAuction di messaggi non richiesti né lo aveva autorizzato. Ai consumatori è anche offerta la possibilità di annullare la loro iscrizione a ReverseAuction e di fare cancellare le informazioni a carattere personale dalla base di dati di questo sito. Inoltre, la sentenza fa obbligo a ReverseAuction di cancellare le informazioni a carattere personale riguardanti gli abbonati di eBay che hanno ricevuto i messaggi di posta elettronica di ReverseAuction senza essere iscritti a questo sito e vieta l'utilizzo o la divulgazione di tali dati. Infine, conformemente alle decisioni precedenti ottenute dalla FTC in materia di tutela della sfera privata, la sentenza impone a ReverseAuction di diffondere i suoi principi in materia di tutela della sfera privata sul suo sito Internet e contiene disposizioni esaurienti in materia di registrazione dei dati che permettono alla FTC di controllare l'applicazione di tali principi.

Il caso ReverseAuction dimostra che la FTC è determinata ad adottare misure d'esecuzione per rafforzare i codici d'autoregolamentazione applicati dalle imprese per quanto riguarda la tutela della sfera privata dei consumatori su Internet. In questo caso sono state messe direttamente sotto accusa pratiche incompatibili con un accordo per la tutela della sfera privata e tali da minare la fiducia dei consumatori nelle misure di protezione adottate dalle società di vendita su Internet. Poiché riguarda l'appropriazione abusiva da parte di un'impresa di informazioni a carattere personale protette da principi di protezione stabiliti da un'altra impresa, questo caso può anche assumere particolare rilevanza in relazione ai problemi di tutela della sfera privata posti dal trasferimento di dati tra imprese di vari paesi.

Anche se la Commissione federale del commercio ha intrapreso azioni coercitive nei casi di GeoCities Liberty Financial Cos. e ReverseAuction, la sua competenza è più limitata in alcuni settori della tutela della sfera privata su Internet. Come si è già osservato, le informazioni a carattere personale raccolte e utilizzate senza l'accordo delle persone interessate rientrano nel campo d'applicazione del FTC Act soltanto se costituiscono pratiche commerciali sleali o fraudolente. Di conseguenza, il FTC Act non si applica alle pratiche di un sito web che raccolga informazioni a carattere personale presso i consumatori senza celare lo scopo per il quale le informazioni sono raccolte né utilizzare o diffondere questi dati in modo da arrecare grave danno ai consumatori. Inoltre, la FTC non ha attualmente sempre il potere di esigere in via generale dalle entità che raccolgono informazioni su Internet di adottare una politica di tutela della sfera privata (9). Tuttavia, come si è detto, un'impresa che non rispetta i suoi impegni in materia di tutela della sfera privata può per ciò stesso commettere un atto fraudolento.

(9) Per questa ragione la Commissione federale del commercio ha dichiarato, nel quadro di un'udienza dinanzi al Congresso, che testi legislativi supplementari sarebbero probabilmente necessari per costringere tutti i siti Internet americani di carattere commerciale rivolti ai consumatori ad attenersi a pratiche precise per quanto riguarda la corretta informazione. «Consumer Privacy on the World Wide Web», documento presentato il 21 luglio 1998 alla sottocommissione delle telecomunicazioni, del commercio e della tutela dei consumatori della commissione del commercio della Camera dei rappresentanti degli Stati Uniti; questo documento può essere consultato in: www.ftc.gov/os/9807/privac98.htm. La FTC non ha ancora chiesto l'elaborazione di tale legislazione affinché le imprese che optano per codici d'autoregolamentazione possano dimostrare che le buone pratiche in materia d'informazione nei siti web sono largamente diffuse. Nella relazione sulla tutela della sfera privata su Internet presentata al Congresso nel giugno 1998 («Privacy Online: A Report to Congress»), il documento può essere consultato in: www.ftc.gov/reports/privacy3/toc.htm, la FTC ha raccomandato l'adozione di testi legislativi che impongano ai siti web commerciali di ottenere l'accordo dei genitori prima di raccogliere informazioni a carattere personale presso bambini di meno di 13 anni (cfr. nota 3 supra). L'anno scorso la FTC ha constatato, nella sua relazione «Self-Regulation and Privacy Online. A Federal Trade Commission Report to Congress» (luglio 1999; il documento può essere consultato in: www.ftc.gov/os/1999/9907/index.htm#13), che progressi soddisfacenti sono stati raggiunti in materia d'autoregolamentazione e, di conseguenza, ha deciso di non raccomandare l'elaborazione di testi di legge.
Nel maggio 2000 la Commissione ha pubblicato una terza relazione al Congresso, «Privacy Online: Fair Information Practices in the Electronic Marketplace» (www.ftc.gov/os/2000/05/index.htm#22), in cui è esaminata la recente indagine della FTC sui siti web commerciali e sul loro rispetto di pratiche informative corrette. La relazione ha anche raccomandato (a maggioranza della Commissione) che il Congresso emani una legislazione che assicuri un livello di base di protezione della privacy per i siti web commerciali orientati ai consumatori.

Inoltre, la competenza della FTC in questo campo si esercita sulle sole pratiche sleali o fraudolente di natura «commerciale». Le informazioni raccolte da entità commerciali che promuovono prodotti o servizi, comprese le informazioni raccolte e utilizzate a fini commerciali, corrispondono presumibilmente a questo requisito. D'altra parte, in molti casi privati le entità raccolgono informazioni su Internet senza perseguire un obiettivo commerciale e quindi non rientrano nell'ambito di competenza della FTC. Si possono citare, come esempio, le «chat rooms» gestite da entità non commerciali, in particolare da organismi d'utilità pubblica.

Occorre infine notare che alcune esclusioni legali totali o parziali dall'ambito di competenza fondamentale della FTC in materia di pratiche commerciali limitano la capacità della FTC di dare una risposta esauriente ai problemi di tutela della sfera privata su Internet. Queste esclusioni riguardano numerose imprese che fanno largamente ricorso alle informazioni sui consumatori come le banche, le società d'assicurazione e le compagnie aeree. Come Lei sa, queste entità sono di competenza di altre agenzie a livello federale o al livello degli Stati, come le agenzie federali incaricate delle questioni bancarie e il ministero dei trasporti.

Nei casi che sono di sua competenza, la FTC riceve e, risorse permettendo, istruisce le denunce pervenute dai consumatori [per posta elettronica, per telefono e ora anche sul suo sito web (10)] presso il suo centro di risposta ai consumatori (CRC). Il CRC riceve le denunce di tutti i consumatori, anche di quelli che risiedono negli Stati membri dell'Unione europea. Il FTC Act permette alla Commissione federale del commercio di imporre misure cautelative contro future infrazioni di tale legge e la riparazione dei danni subiti dai consumatori. Cerchiamo tuttavia di accertare se l'impresa segue un modello di comportamento inappropriato, poiché non trattiamo i singoli contenziosi con i consumatori. In passato, la Commissione federale del commercio ha ottenuto riparazioni per cittadini degli Stati Uniti e di altri paesi (11). La FTC continuerà, nei casi appropriati, ad imporre la sua autorità per ottenere riparazioni per i cittadini di altri paesi che abbiano subito un danno in seguito a pratiche fraudolente che rientrano nell'ambito della propria competenza.

*Dati sull'occupazione*

Nella Sua ultima lettera, Lei ha chiesto precisazioni supplementari sulle attribuzioni della FTC nel settore dei dati sull'occupazione. In primo luogo, chiede se la FTC può intervenire, in virtù della sezione 5, contro un'impresa che afferma di attenersi ai principi «approdo sicuro», ma trasferisce o utilizza dati sull'occupazione in modo contrario a questi principi. Desideriamo garantirLe che abbiamo accuratamente esaminato le disposizioni legislative che definiscono il mandato del FTC, i documenti connessi e la giurisprudenza, e che abbiamo concluso che la FTC ha per i dati relativi all'occupazione la stessa competenza che ha in generale in virtù della sezione 5 del FTC Act (12). In altri termini, nel caso in cui siano soddisfatti gli attuali criteri che giustificano un'azione a tutela della sfera privata (pratiche sleali e fraudolente) possiamo intervenire in situazioni che implicano dati relativi all'occupazione.

Desideriamo anche dissipare i dubbi che potrebbero esistere quanto alla capacità della FTC di adottare misure d'esecuzione soltanto nei casi in cui un'impresa abbia ingannato singoli consumatori. In realtà, come l'azione della FTC nell'affare ReverseAuction (13) dimostra chiaramente, la FTC avvia un procedimento esecutivo a tutela della sfera privata quando, nel quadro di trasferimenti di dati tra imprese, una delle imprese interessate agisce illecitamente nei confronti di un'altra impresa, con eventuale danno per i consumatori e le imprese stesse. Pensiamo che si tratti della situazione in cui è più probabile che si ponga la questione dei dati sull'occupazione, poiché i dati di questo tipo riguardanti cittadini europei sono trasferiti da imprese europee a imprese americane che hanno assunto l'impegno di rispettare i principi dell'approdo sicuro.

Desideriamo tuttavia segnalare che, in alcune circostanze, la possibilità d'azione della FTC è limitata, in particolare quando un affare è già trattato nel quadro di una controversia tradizionale di diritto del lavoro, abitualmente un reclamo o una domanda d'arbitrato o anche una denuncia presso il «National Labor Relations Board» di pratiche fraudolente nel settore del diritto del lavoro. Questo sarebbe il caso, ad esempio, se un datore di lavoro avesse assunto un

(10) Cfr. http://www.ftc.gov/ftc/complaint.htm per il modulo online di denuncia della Commissione federale del commercio.

(11) Ad esempio, in un recente caso di piramide finanziaria su Internet, la FTC ha ottenuto rimborsi di una somma totale di circa 5,5 milioni di USD per 15 622 consumatori, residenti negli Stati Uniti e in 70 paesi stranieri (cf. www.ftc.gov/opa/9807/fortunar.htm; www.ftc.gov/opa/9807/ftcrefund01.htm).

(12) Tranne nei casi esplicitamente esclusi nello statuto della FTC, le competenze che il FTC Act conferisce alla FTC in relazione a pratiche «commerciali o riguardanti il commercio» coesistono con i poteri costituzionali del Congresso ai sensi della clausola sul commercio [United States v. American Building Maintenance Industries, 422 U.S. 271, 277 n. 6 (1975)]. La sfera di competenza della FTC include dunque le pratiche adottate in materia d'occupazione dalle imprese e dalle industrie nel commercio internazionale.

(13) Cfr. «Online Auction Site Settles FTC Privacy Charges», FTC News Release (6 gennaio 2000) disponibile in: http://www.ftc.gov/opa/2000/01/reverse4.htm.

impegno circa l'utilizzo di dati a carattere personale nel quadro di un accordo collettivo e un lavoratore dipendente o un sindacato sostenesse che il datore di lavoro non rispetta tale accordo. La FTC si rimetterebbe probabilmente a tale procedura [14].

*Competenza in materia di «sistemi d'omologazione»*

In secondo luogo, Lei chiede se la FTC sia competente per quanto riguarda i sistemi di «omologazione» (seal programs) che permettono di gestire meccanismi di risoluzione delle controversie negli Stati Uniti, quando tali sistemi vengono meno al loro ruolo nel garantire l'applicazione dei principi dell'approdo sicuro e nel trattare i singoli reclami, anche se — tecnicamente — questi sistemi sono organismi senza scopo di lucro. Per determinare se un'entità che dichiara di non avere scopo di lucro è di competenza della FTC, esaminiamo accuratamente se quest'entità, pur non perseguendo un profitto per sé, non persegua un profitto per i suoi membri. La Commissione ha fatto valere la propria competenza in questo settore e la Corte suprema degli Stati Uniti ha del resto dichiarato all'unanimità, il 24 maggio 1999, che la FTC aveva giurisdizione su un'associazione privata senza scopo di lucro che riunisce gruppi locali di odontoiatri in una causa antitrust (California Dental Association v. Federal Trade Commission). La Corte ha ritenuto che:

> Il FTC Act deve riguardare non soltanto le entità «organizzate per svolgere un'attività per il proprio profitto» (15 U.S.C. § 44), ma anche le entità che mirano ad ottenere profitti per conto «dei loro membri». (…) È infatti difficile supporre che il Congresso abbia inteso in senso così restrittivo le organizzazioni di supporto, dato che questo permetterebbe di sottrarsi alla giurisdizione della FTC in casi in cui le finalità del FTC Act richiederebbero di imporla.

In sostanza, per determinare se ha giurisdizione su un'entità particolare «senza scopo di lucro» che gestisce un sistema d'omologazione, la Commissione federale del commercio deve esaminare concretamente in quale misura tale entità permette ai suoi membri di conseguire un profitto. Se tale entità gestisce il suo sistema d'omologazione in modo da ottenere profitti per i suoi membri, è probabile che la FTC si dichiari competente. D'altra parte, la FTC avrebbe probabilmente giurisdizione su un sistema fraudolento che si presenti falsamente come entità senza scopo di lucro.

*Tutela dei dati a carattere personale «offline»*

In terzo luogo, Lei osserva che la nostra precedente corrispondenza riguardava principalmente la tutela della sfera privata nel quadro delle attività «online». Se questo settore costituisce una delle preoccupazioni principali della FTC, in quanto elemento cruciale dello sviluppo del commercio elettronico, il FTC Act risale al 1914 e si applica anche alle attività «offline». Possiamo perciò avviare azioni nei confronti di imprese che adottano pratiche commerciali sleali o fraudolente in relazione alla tutela della sfera privata dei consumatori [15]. In un caso sottoposto l'anno scorso alla FTC (FTC v. TouchTone Information, Inc.) un «intermediario di informazione» è stato incaricato di ottenere e vendere illegalmente dati riservati sulla situazione finanziaria di alcuni consumatori. La FTC ha sostenuto che TouchTone aveva ottenuto queste informazioni adducendo vari pretesti, utilizzando tecniche in uso tra gli investigatori privati per ottenere informazioni a carattere personale, generalmente per telefono. In questa causa, registrata il 21 aprile 1999 presso una Corte federale del Colorado, sono state richieste un'ingiunzione e la restituzione dei guadagni ottenuti illegalmente.

Questa esperienza di applicazione della legge, come pure le inquietudini sollevate di recente dalla fusione di basi dati offline e online e il fatto che una gran quantità di dati a carattere personale sono raccolti e utilizzati offline, spiegano perché sia prestata particolare attenzione alle questioni riguardanti la privacy offline.

*Sovrapposizione di competenze*

Infine, Lei solleva la questione della possibile sovrapposizione di competenze tra la FTC e le altre agenzie interessate. Abbiamo rapporti di stretta cooperazione con numerose altre agenzie, anche con le agenzie federali di sorveglianza

(14) Per determinare se una pratica è contraria al diritto del lavoro o se costituisce una violazione di un accordo collettivo occorre un esame tecnico che abitualmente è compito dei tribunali del lavoro che istruiscono le denunce, in particolare gli organi arbitrali e il National Labor Relations Board (NLRB).

(15) Come Lei sa, il «Fair Credit Reporting Act» dà anche alla FTC il potere di tutelare la riservatezza dei dati personali a carattere finanziario nel quadro dell'applicazione della legge e la commissione ha recentemente preso una decisione sulla questione. Cf. In the Matter of Trans Union, Docket No. 9255, 1º marzo 2000, comunicato stampa e pareri disponibili in: www.ftc.gov/os/2000/03/index.htm#1.

delle attività bancarie e i procuratori generali degli Stati. Coordiniamo spesso le indagini per sfruttare al massimo le nostre risorse nei casi di sovrapposizione di competenze. Inoltre, sottoponiamo spesso questioni all'esame delle agenzie federali o delle agenzie degli Stati.

Spero che questa rassegna Le sia d'utilità e resto a Sua disposizione per ogni altra informazione.

Distinti saluti.

Robert Pitofsky

———

*ALLEGATO VI*

John Mogg
Direttore, DG XV
Commissione europea
Ufficio C 107-6/72
Rue de la Loi/Wetstraat 200
B-1049 Bruxelles

Signor Direttore generale,

Le invio questa lettera su richiesta del Dipartimento del commercio degli Stati Uniti per chiarire il ruolo del Dipartimento dei trasporti nella protezione della sfera privata dei consumatori per quanto riguarda le informazioni da loro comunicate alle società di navigazione aerea.

Il Dipartimento dei trasporti incoraggia l'autoregolamentazione, che considera lo strumento meno importuno e più efficace per garantire la tutela dei dati di carattere privato forniti dai consumatori alle compagnie aeree e, di conseguenza, è favorevole all'istituzione di un regime di «approdo sicuro» che permetta alle compagnie aeree di conformarsi alle disposizioni della direttiva europea sulla protezione dei dati personali per quanto riguarda i trasferimenti di dati al di fuori dell'UE. Il Dipartimento riconosce tuttavia che, per garantire l'efficacia di questi sforzi di autoregolamentazione, è essenziale che le compagnie aeree che s'impegnano a osservare i principi stabiliti dal regime «approdo sicuro» li rispettino effettivamente. A questo riguardo, l'autoregolamentazione dovrebbe essere integrata da misure che ne garantiscano l'applicazione effettiva. Pertanto, facendo ricorso alla sua esistente autorità statutaria di protezione dei consumatori, il Dipartimento garantirà che le compagnie aeree rispettino gli impegni presi nei confronti del pubblico per quanto riguarda la protezione della sfera privata ed esaminerà le denunce di inosservanza pervenute dalle organizzazioni di autoregolamentazione e da altri, compresi gli Stati membri dell'Unione europea.

Il Dipartimento ha l'autorità di prendere misure di esecuzione in questo campo in virtù di quando disposto dalla norma 49 U.S.C. 41712, che fa divieto a un trasportatore di ricorrere a «pratiche sleali o ingannevoli o a forme sleali di concorrenza» nella vendita di prestazioni di trasporto aereo che comportino o possano comportare un danno per il consumatore. La sezione 41712 è modellata sulla sezione 5 della legge sulla Commissione federale del commercio (Federal Trade Commission Act, 15 U.S.C. 45). Tuttavia, i trasportatori aerei sono esonerati dalle disposizioni della sezione 5 dalla Commissione federale del commercio ai sensi di 15 U.S.C. 45(a)(2).

I miei servizi svolgono indagini e ricorrono in giudizio ai sensi di 49 U.S.C. 41712 (cfr. ad esempio, le seguenti ordinanze del Dipartimento dei trasporti: 99-11-5, 9 novembre 1999; 99-8-23, 26 agosto 1999; 99-6-1, 1º giugno 1999; 98-6-24, 22 giugno 1998; 98-6-21, 19 giugno 1998; 98-5-31, 22 maggio 1998 e 97-12-23, 18 dicembre 1997). I procedimenti di questo tipo sono istruiti in base alle nostre indagini e a reclami ufficiali o informali presentati da privati, agenzie di viaggi, compagnie aeree e organi amministrativi americani o stranieri.

Vorrei richiamare la Vostra attenzione sul fatto che il mancato rispetto da parte di un trasportatore del carattere privato delle informazioni comunicate da un passeggero non costituirebbe di per sé una violazione della sezione 41712. Tuttavia, se un trasportatore si è formalmente e pubblicamente impegnato a conformarsi ai principi «approdo sicuro» relativi alla protezione del carattere riservato delle informazioni fornitegli dal consumatore, il Dipartimento ha facoltà di far uso dei poteri che gli sono conferiti dalla sezione 41712 per garantire il rispetto di questi principi. Di conseguenza, quando un passeggero comunica informazioni ad un trasportatore che si è impegnato a rispettare i principi «approdo sicuro», ogni inadempimento di quest'impegno può arrecare pregiudizio al consumatore e costituisce una violazione della sezione 41712. I miei servizi attribuiscono la massima importanza all'esame di attività di questo tipo e all'apertura di procedimenti per casi riguardanti attività di questo tipo. Informiamo anche il Dipartimento del commercio dei risultati di queste azioni.

L'inosservanza delle disposizioni della sezione 41712 può dar luogo a ordinanze e a sanzioni civili in caso di violazione di queste ordinanze. Anche se non abbiamo l'autorità di imporre il risarcimento dei danni o una riparazione pecuniaria al querelante, possiamo approvare gli accomodamenti risultati dalle indagini e dalle cause istruite dal Dipartimento che prevedono indennizzi a titolo di riparazione o come compensazione di sanzioni pecuniarie altrimenti pagabili. Abbiamo proceduto così in passato e continuiamo e continueremo a farlo nel quadro dei principi «approdo sicuro» quando le circostanze lo giustificano. Infrazioni ripetute alla sezione 41712 da parte di una società aerea americana solleverebbero anche dubbi sulla sua volontà di rispettare il suo impegno e, in situazioni estreme, potrebbero portare il ritiro dell'autorizzazione di esercizio e, quindi, alla perdita dell'abilitazione ad esercitare un'attività economica. [Cfr. le ordinanze del Dipartimento dei trasporti 93-6-34, 23 giugno 1993 e 93-6-11, 9 giugno 1993. Benché la causa non riguardasse la

sezione 41712, si è conclusa con la revoca a un trasportatore dell'autorizzazione di esercizio per violazione grave delle disposizioni della legge federale sul trasporto aereo (Federal Aviazione Act), di un accordo bilaterale e delle norme e dei regolamenti del Dipartimento.]

Spero che queste informazioni vi siano utili e resto a vostra disposizione per ogni altra informazione.

Distinti saluti

Samuel Podberesky

Assistant General Counsel for
Aviation Enforcement and Proceeding

---

*ALLEGATO VII*

In riferimento all'articolo 1, paragrafo 2, lettera b), gli enti governativi degli Stati Uniti autorizzati all'istruttoria delle denunce e a ottenere riparazione per pratiche sleali o ingannevoli, anche nel caso di singoli individui, indipendentemente dal paese di residenza o di nazionalità degli individui stessi, in materia di mancato rispetto dei principi applicati conformemente alle FAQ, sono:

1. la Commissine federale per il commercio, e

2. il Dipartimento dei trasporti.

La competenza della Commissione federale per il commercio si fonda sulla sezione 5 del Federal Trade Commission Act. La competenza della Commissione federale per il commercio in materia di atti o pratiche sleali o ingannevoli è esclusa per quanto riguarda banche, casse di risparmio e istituti di credito; vettori di telecomunicazioni e di trasporti comuni interstatali, vettori e portatori aerei e operatori di recinti per bestiame. Benché l'industria assicurativa non sia specificatamente compresa nell'elenco delle eccezioni di cui alla sezione 5, il McCarran-Ferguson Act (1) in generale demanda la regolamentazione delle imprese di assicurazioni ai singoli Stati. Tuttavia, le disposizioni del Federal Trade Commission Act si applicano all'industria assicurativa nella misura in cui tale industria non è soggetta alla legislazione degli Stati. Analogamente, la Federal Trade Commission dispone di una competenza residuale in merito a pratiche sleali o ingannevoli da parte di compagnie d'assicurazione quando non siano impegnate in attività assicurative.

La competenza del Dipartimento dei trasporti degli Stati Uniti si fonda sul titolo 49 della sezione 41712 dell'United States Code. Il Dipartimento dei trasporti degli Stati Uniti istruisce i casi sulla base di proprie investigazioni nonché di denunce formali e informali recevute da singoli individui, agenti di viaggio, compagnie aeree, ed enti governativi degli Stati Uniti e stranieri.

---

(1) 15 U.S.C., paragrafo 1011 e segg.

**01A11980**

DELIBERAZIONE 17 ottobre 2001.

**Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso la Svizzera, in conformità a quanto previsto dalla decisione della Commissione europea del 26 luglio 2000, n. 2000/518/CE.** (Deliberazione n. 37).

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del Prof. Stefano Rodotà, presidente, del Prof. Giuseppe Santaniello, vice-presidente, del Prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 25, paragrafi nn. 1 e 2, della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 secondo cui i dati personali possono essere trasferiti in un Paese non appartenente all'Unione europea qualora il Paese terzo garantisca un livello di protezione adeguato, secondo quanto previsto nel paragrafo 2 del medesimo articolo;

Visto il paragrafo 6 del medesimo art. 25 secondo il quale la Commissione europea può constatare che un Paese terzo garantisce un livello di protezione adeguato ai sensi del citato paragrafo 2, ai fini della tutela della vita privata o dei diritti e delle libertà fondamentali della persona;

Vista la decisione della Commissione europea del 26 luglio 2000 n. 2000/518/CE (pubblicata sulla *Gazzetta Ufficiale delle Comunità europee* L 215 del 25 agosto 2000 e L 115 del 25 aprile 2001) con la quale si è constatato che la Svizzera garantisce un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea;

Considerato che gli Stati membri europei devono adottare le misure necessarie per conformarsi alla decisione della Commissione, ai sensi del paragrafo 6 del citato art. 25 della direttiva;

Visto l'art. 28 della legge 31 dicembre 1996, n. 675 secondo cui il trasferimento dei dati personali all'estero può avvenire: *a*) qualora l'ordinamento dello Stato di destinazione o di transito dei dati assicuri un livello di tutela delle persone adeguato o, se si tratta di dati sensibili o di taluni dati di carattere giudiziario, di grado pari a quello assicurato dall'ordinamento italiano; *b*) oppure, qualora ricorra uno dei casi previsti nel comma 4 del medesimo articolo; *c*) in ogni caso, qualora sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto (comma 4, lett. g));

Ritenuta la necessità di adottare una misura necessaria per l'applicazione della Decisione della Commissione in conformità al citato art. 28, nelle more del completamento del recepimento della citata direttiva n. 95/46/CE;

Ritenuto che le disposizioni di rango costituzionale e le altre norme vigenti in Svizzera in materia di protezione dei dati personali, valutate dalla Commissione e anche dal Gruppo delle autorità garanti europee di cui all'art. 29 della citata direttiva, prevedono diverse garanzie per i diritti dell'interessato che in conformità al diritto comunitario vanno ritenute adeguate ai sensi del citato art. 28, comma 4, lett. g);

Rilevato che la Decisione della Commissione può essere adattata alla luce dell'esperienza acquisita nel corso della sua applicazione o di innovazioni intervenute nell'ordinamento svizzero (art. 4);

Visti gli articoli 2 e 3 della Decisione in tema di controlli e provvedimenti delle autorità di garanzia degli Stati membri sulla liceità e correttezza dei trasferimenti e dei trattamenti di dati anteriori ai trasferimenti medesimi, anche in relazione a quanto previsto dall'articolo 4 della direttiva n. 95/46/CE sul diritto nazionale applicabile;

Ritenuta la necessità di assicurare ulteriore pubblicità alla predetta Decisione disponendo la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana in allegato alla presente autorizzazione;

Vista la documentazione d'ufficio;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il prof. Gaetano Rasi;

TUTTO CIO' PREMESSO IL GARANTE:

1) autorizza i trasferimenti di dati personali dal territorio dello Stato verso la Svizzera, in conformità a quanto previsto dalla Decisione della Commissione europea del 26 luglio 2000 n. 2000/518/CE;

2) si riserva, in conformità alla normativa comunitaria, alla legge n. 675/1996 e agli artt. 2 e 3 della Decisione della Commissione, di svolgere i necessari controlli sulla liceità e correttezza dei trasferimenti di dati e delle operazioni di trattamento anteriori ai trasferimenti medesimi, e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento;

3) dispone la trasmissione del presente provvedimento e dell'allegata decisione della Commissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica Italiana.

Roma, 17 ottobre 2001

*Il presidente:* RODOTÀ

*Il relatore:* RASI

*Il segretario generale:* BUTTARELLI

II

*(Atti per i quali la pubblicazione non è una condizione di applicabilità)*

# COMMISSIONE

## DECISIONE DELLA COMMISSIONE

**del 26 luglio 2000**

**riguardante l'adeguatezza della protezione dei dati personali in Svizzera a norma della direttiva 95/46/CE**

*[notificata con il numero C(2000) 2304]*

**(Testo rilevante ai fini del SEE)**

(2000/518/CE)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [1], in particolare l'articolo 25, paragrafo 6,

considerando quanto segue:

(1) La direttiva 95/46/CE prescrive agli Stati membri di assicurarsi che i trasferimenti di dati personali verso un determinato paese terzo abbiano luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato e se le leggi dello Stato membro che attuano le altre disposizioni della direttiva sono rispettate prima del trasferimento.

(2) La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. Tale constatazione permette il trasferimento di dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.

(3) A norma della direttiva 95/46/CE l'adeguatezza del livello di protezione dei dati personali deve essere valutata con riguardo a tutte le circostanze relative a un trasferimento o a una categoria di trasferimenti di dati e nel rispetto di determinate condizioni. Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali, istituito a norma della direttiva, ha fornito indicazioni sull'effettuazione di tali valutazioni [2].

(4) Tenuto conto dei distinti modi in cui vengono protetti i dati nei paesi terzi, sia la verifica dell'adeguatezza di tale protezione, sia l'applicazione di ogni decisione basata sull'articolo 25, paragrafo 6, della direttiva 95/46/CE, devono avvenire in modo da non produrre discriminazioni arbitrarie o ingiustificate nei confronti di o tra paesi terzi in cui sussistono condizioni analoghe e da non costituire ostacoli occulti agli scambi, tenendo conto degli attuali impegni internazionali della Comunità.

(5) Nella Confederazione svizzera vigono in materia di protezione dei dati personali norme di legge che producono effetti giuridici vincolanti a livello federale e cantonale.

(6) La costituzione federale, modificata in seguito alla consultazione popolare del 18 aprile 1999 ed entrata in vigore il 1º gennaio 2000, garantisce a ciascun cittadino il diritto al rispetto della vita privata e, in particolare, il diritto di essere tutelato contro l'uso illecito dei dati che lo riguardano. Il tribunale federale ha sviluppato, sulla base della precedente costituzione che non prevedeva una siffatta disposizione, una giurisprudenza che fissa i principi generali applicabili al trattamento dei dati perso-

[1] GU L 281 del 23.11.1995, pag. 31.

[2] Parere 12/98, adottato dal gruppo di lavoro il 24 luglio 1998: «Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati» (DG MARKT D/5025/98), disponibile sul sito «Europa» della Commissione europea al seguente indirizzo: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

nali con riguardo, in particolare, alla qualità dei dati trattati, al diritto di accesso degli interessati e al diritto di chiedere la rettifica o la distruzione dei dati. Tali principi sono vincolanti tanto per la federazione quanto per ciascun cantone.

(7) La legge federale svizzera sulla protezione dei dati del 19 giugno 1992 è entrata in vigore il 1º luglio 1993. Le modalità di applicazione di talune disposizioni della legge, riguardanti in particolare il diritto di accesso delle persone interessate, la notifica dei trattamenti all'autorità di controllo indipendente e la comunicazione di dati all'estero, sono state fissate mediante ordinanze del Consiglio federale. La legge si applica ai trattamenti di dati personali effettuati da organi federali e da tutto il settore privato nonché ai trattamenti effettuati da organi cantonali in applicazione del diritto federale nella misura in cui tali trattamenti non sono soggetti a disposizioni cantonali di protezione dei dati.

(8) Nella maggioranza dei casi i cantoni hanno adottato un atto legislativo in materia di protezione dei dati per i settori di loro competenza quali, in particolare, ospedali pubblici, istruzione, imposte dirette cantonali e polizia. Negli altri cantoni, tali trattamenti sono disciplinati da atti di natura regolamentare o secondo i principi della giurisprudenza cantonale. Quali che siano la fonte e il contenuto delle disposizioni cantonali, e anche in assenza di disposizioni cantonali, i cantoni devono conformarsi ai principi costituzionali sopra citati. È possibile che le autorità cantonali, nei settori di loro competenza, debbano trasferire dati personali alle amministrazioni pubbliche di Stati limitrofi essenzialmente a fini di reciproca assistenza per la tutela di interessi pubblici rilevanti o, nel caso degli ospedali pubblici, al fine di tutelare l'interesse fondamentale delle persone in questione.

(9) Il 2 ottobre 1997 la Svizzera ha ratificato la convenzione del Consiglio d'Europa sulla protezione delle persone riguardo al trattamento automatizzato di dati di carattere personale (convenzione n. 108) [3], volta a rafforzare la tutela dei dati personali e ad assicurare la libera circolazione tra le parti contraenti, fatte salve le deroghe da queste eventualmente previste. Pur senza essere direttamente applicabile, la convenzione definisce gli obblighi internazionali sia della Federazione, sia dei cantoni per quanto riguarda non soltanto i principi fondamentali della protezione che ciascuna parte contraente deve attuare nel suo diritto interno, ma anche i meccanismi di cooperazione tra le parti contraenti. In particolare, le competenti autorità svizzere devono fornire alle autorità delle altre parti contraenti che ne fanno richiesta ogni informazione sul diritto e sulle prassi amministrative in materia di protezione dei dati nonché informazioni relative ad ogni caso specifico di trattamento automatizzato di dati. Inoltre, esse devono prestare assistenza alle persone residenti all'estero nell'esercizio del loro diritto di essere informate circa l'esistenza di un trattamento di dati che le riguardano, del diritto di accedere ai dati che le riguardano e di chiederne la rettifica o la cancellazione, nonché del diritto di proporre un ricorso giurisdizionale.

(10) Le norme di legge vigenti in Svizzera incorporano tutti i principi fondamentali necessari per assicurare un livello di protezione adeguato delle persone fisiche, anche se eccezioni e limitazioni sono previste a salvaguardia di interessi pubblici rilevanti. L'applicazione di tali norme è garantita dai ricorsi giurisdizionali nonché dal controllo indipendente esercitato dalle autorità, quali l'incaricato federale investito di poteri di indagine e di intervento. In caso di trattamenti illeciti arrecanti pregiudizio alla persona interessata si applicano inoltre le disposizioni della legge svizzera in materia di responsabilità civile.

(11) Nell'interesse della trasparenza e al fine di salvaguardare la capacità delle autorità competenti negli Stati membri di garantire la tutela delle persone fisiche per quanto concerne il trattamento dei dati personali che li riguardano, è necessario specificare nella decisione le circostanze eccezionali in cui, nonostante la constatazione di un livello di protezione adeguato, può essere giustificata la sospensione di trasferimenti di dati specifici.

(12) Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE si è pronunciato sul livello di protezione garantito dalla legislazione elvetica. In sede di elaborazione della presente decisione si è tenuto conto del parere espresso da tale gruppo [4].

(13) Le misure previste dalla presente decisione sono conformi al parere del comitato istituito dall'articolo 31 della direttiva 95/46/CE,

HA ADOTTATO LA PRESENTE DECISIONE:

*Articolo 1*

Ai fini dell'applicazione dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, si considera per tutte le attività che rientrano nel campo d'applicazione della direttiva, che la Svizzera offra un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea.

*Articolo 2*

La presente decisione riguarda soltanto l'adeguatezza della protezione garantita in Svizzera in base ai requisiti prescritti dal-

[3] http://conventions.coe.int/treaty/EN/cadreintro.htm.

[4] Parere 5/99, adottato dal gruppo di lavoro il 7 giugno 1999 (GD MARKT 5054/99), disponibile sul sito Web «Europa» della Commissione europea all'indirizzo indicato nella nota 2.

l'articolo 25, paragrafo 1, della direttiva 95/46/CE e non incide su condizioni o restrizioni stabilite in applicazione di altre disposizioni della direttiva relativamente al trattamento di dati personali negli Stati membri.

*Articolo 3*

1. Fatta salva la loro facoltà di prendere provvedimenti per garantire l'osservanza delle disposizioni nazionali adottate in conformità a disposizioni diverse da quelle di cui all'articolo 25 della direttiva 95/46/CE, le autorità competenti degli Stati membri possono esercitare i poteri di cui dispongono per sospendere trasferimenti di dati diretti ad un destinatario in Svizzera al fine di tutelare gli interessati in relazione al trattamento dei dati personali che li riguardano nei casi in cui:

a) la competente autorità svizzera abbia accertato che il destinatario viola le norme vigenti in materia di protezione, oppure

b) sia molto probabile una violazione delle norme di protezione; vi siano validi motivi per ritenere che la competente autorità svizzera non stia adottando o non adotterà misure adeguate e tempestive per risolvere il caso in questione; la continuazione del trasferimento comporti un rischio imminente di gravi danni per gli interessati e le autorità competenti degli Stati membri abbiano fatto il possibile, date le circostanze, per informare il soggetto stabilito in Svizzera che è responsabile del trattamento dei dati, dandogli la possibilità di replicare.

La sospensione cessa non appena sia garantito il rispetto delle norme di protezione e sia stata informata l'autorità competente della Comunità.

2. Gli Stati membri informano senza indugio la Commissione dell'adozione di misure in base al paragrafo 1.

3. Gli Stati membri e la Commissione si informano anche reciprocamente dei casi in cui le misure adottate dagli organismi incaricati di vigilare sul rispetto delle norme di protezione in Svizzera risultano inidonee a tal fine.

4. Se le informazioni raccolte in applicazione dei paragrafi 1, 2 e 3 dimostrano che uno degli organismi incaricati di vigilare sul rispetto delle norme di protezione in Svizzera non assolve efficacemente la sua funzione, la Commissione informa l'autorità svizzera competente e, se necessario, presenta un progetto delle misure da adottare secondo la procedura di cui all'articolo 31 della direttiva al fine di abrogare o sospendere la presente decisione o limitarne il campo d'applicazione.

*Articolo 4*

1. La presente decisione può essere modificata in qualsiasi momento alla luce dell'esperienza acquisita nel corso della sua applicazione o di emendamenti apportati alla legislazione svizzera.

La Commissione valuta l'applicazione della presente decisione, sulla base delle informazioni disponibili, tre anni dopo la sua notifica agli Stati membri e riferisce ogni risultanza al comitato istituito a norma dell'articolo 31 della direttiva 95/46/CE, incluso ogni elemento che possa influire sulla valutazione di cui all'articolo 1 della presente decisione circa l'adeguatezza della protezione in Svizzera ai sensi dell'articolo 25 della direttiva 95/46/CE e ogni elemento da cui risulti che la decisione è applicata in modo discriminatorio.

2. La Commissione, se necessario, presenta un progetto delle misure da adottare conformemente alla procedura di cui all'articolo 31 della direttiva 95/46/CE.

*Articolo 5*

Gli Stati membri adottano le misure necessarie per conformarsi alla presente decisione entro novanta giorni dalla data della sua notifica agli Stati membri.

*Articolo 6*

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 26 luglio 2000.

*Per la Commissione*
Frederik BOLKESTEIN
*Membro della Commissione*

**01A11981**

DELIBERAZIONE 17 ottobre 2001.

**Autorizzazione al trasferimento di dati personali dal territorio dello Stato verso l'Ungheria, in conformità a quanto previsto dalla decisione della Commissione europea del 26 luglio 2000, n. 2000/519/CE.** (Deliberazione n. 38).

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del Prof. Stefano Rodotà, presidente, del Prof. Giuseppe Santaniello, vice-presidente, del Prof. Gaetano Rasi e del dott. Mauro Paissan, componenti e del dott. Giovanni Buttarelli, segretario generale;

Visto l'art. 25, paragrafi nn. 1 e 2, della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 secondo cui i dati personali possono essere trasferiti in un Paese non appartenente all'Unione europea qualora il Paese terzo garantisca un livello di protezione adeguato, secondo quanto previsto nel paragrafo 2 del medesimo articolo;

Visto il paragrafo 6 del medesimo art. 25 secondo il quale la Commissione europea può constatare che un Paese terzo garantisce un livello di protezione adeguato ai sensi del citato paragrafo 2, ai fini della tutela della vita privata o dei diritti e delle libertà fondamentali della persona;

Vista la decisione della Commissione europea del 26 luglio 2000 n. 2000/519/CE (pubblicata sulla *Gazzetta Ufficiale delle Comunità europee* L 215 del 25 agosto 2000 e L 115 del 25 aprile 2001) con la quale si è constatato che l'Ungheria garantisce un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea;

Considerato che gli Stati membri europei devono adottare le misure necessarie per conformarsi alla decisione della Commissione, ai sensi del paragrafo 6 del citato art. 25 della direttiva;

Visto l'art. 28 della legge 31 dicembre 1996, n. 675 secondo cui il trasferimento dei dati personali all'estero può avvenire: *a*) qualora l'ordinamento dello Stato di destinazione o di transito dei dati assicuri un livello di tutela delle persone adeguato o, se si tratta di dati sensibili o di taluni dati di carattere giudiziario, di grado pari a quello assicurato dall'ordinamento italiano; *b*) oppure, qualora ricorra uno dei casi previsti nel comma 4 del medesimo articolo; *c*) in ogni caso, qualora sia autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto (comma 4, lett. g);

Ritenuta la necessità di adottare una misura necessaria per l'applicazione della Decisione della Commissione in conformità al citato art. 28, nelle more del completamento del recepimento della citata direttiva n. 95/46/CE;

Ritenuto che le disposizioni di rango costituzionale e le altre norme vigenti in Ungheria in materia di protezione dei dati personali, valutate dalla Commissione e anche dal Gruppo delle autorità garanti europee di cui all'art. 29 della citata direttiva, prevedono diverse garanzie per i diritti dell'interessato che in conformità al diritto comunitario vanno ritenute adeguate ai sensi del citato art. 28, comma 4, lett. g);

Rilevato che la Decisione della Commissione può essere adattata alla luce dell'esperienza acquisita nel corso della sua applicazione o di innovazioni intervenute nell'ordinamento ungherese (art. 4);

Visti gli articoli 2 e 3 della Decisione in tema di controlli e provvedimenti delle autorità di garanzia degli Stati membri sulla liceità e correttezza dei trasferimenti e dei trattamenti di dati anteriori ai trasferimenti medesimi, anche in relazione a quanto previsto dall'articolo 4 della direttiva n. 95/46/CE sul diritto nazionale applicabile;

Ritenuta la necessità di assicurare ulteriore pubblicità alla predetta Decisione disponendo la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana in allegato alla presente autorizzazione;

Vista la documentazione d'ufficio;

Viste le osservazioni dell'Ufficio, formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante, n. 1/2000;

Relatore il prof. Gaetano Rasi;

TUTTO CIO' PREMESSO IL GARANTE:

1) autorizza i trasferimenti di dati personali dal territorio dello Stato verso l'Ungheria, in conformità a quanto previsto dalla Decisione della Commissione europea del 26 luglio 2000 n. 2000/519/CE;

2) si riserva, in conformità alla normativa comunitaria, alla legge n. 675/1996 e agli artt. 2 e 3 della Decisione della Commissione, di svolgere i necessari controlli sulla liceità e correttezza dei trasferimenti di dati e delle operazioni di trattamento anteriori ai trasferimenti medesimi, e di adottare eventuali provvedimenti di blocco o di divieto di trasferimento;

3) dispone la trasmissione del presente provvedimento e dell'allegata decisione della Commissione all'Ufficio pubblicazione leggi e decreti del Ministero della giustizia per la sua pubblicazione nella *Gazzetta Ufficiale* della Repubblica Italiana.

Roma, 17 ottobre 2001

*Il presidente:* RODOTÀ

*Il relatore:* RASI

*Il segretario generale:* BUTTARELLI

**DECISIONE DELLA COMMISSIONE**

**del 26 luglio 2000**

**riguardante l'adeguatezza della protezione dei dati personali in Ungheria a norma della direttiva 95/46/CE**

*[notificata con il numero C(2000) 2305]*

**(Testo rilevante ai fini del SEE)**

(2000/519/CE)

LA COMMISSIONE DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità europea,

vista la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [1], in particolare l'articolo 25, paragrafo 6,

considerando quanto segue:

(1) La direttiva 95/46/CE prescrive agli Stati membri di assicurarsi che i trasferimenti di dati personali verso un determinato paese terzo abbiano luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato e se le leggi dello Stato membro che attuano le altre disposizioni della direttiva sono rispettate prima del trasferimento.

(2) La Commissione può constatare che un paese terzo garantisce un livello di protezione adeguato. Tale constatazione permette il trasferimento di dati personali dagli Stati membri senza che siano necessarie ulteriori garanzie.

(3) A norma della direttiva 95/46/CE l'adeguatezza del livello di protezione dei dati personali deve essere valutata con riguardo a tutte le circostanze relative a un trasferimento o a una categoria di trasferimenti di dati e nel rispetto di determinate condizioni. Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali, istituito a norma della direttiva, ha fornito indicazioni sull'effettuazione di tali valutazioni [2].

(4) Tenuto conto dei distinti modi in cui vengono protetti i dati nei paesi terzi, sia la verifica dell'adeguatezza di tale protezione, sia l'applicazione di ogni decisione basata sull'articolo 25, paragrafo 6, della direttiva 95/46/CE, devono avvenire in modo da non produrre discriminazioni arbitrarie o ingiustificate nei confronti di o tra paesi terzi in cui sussistono condizioni analoghe e da non costituire ostacoli occulti agli scambi, tenendo conto degli attuali impegni internazionali della Comunità.

(5) In Ungheria vigono in materia di protezione dei dati personali norme di legge che producono effetti giuridici vincolanti.

(6) Il principio della tutela della vita privata, in particolare con riguardo al trattamento dei dati personali, è contemplato dalla costituzione ungherese (articolo 59). Le disposizioni legislative sono fissate dalla legge LXIII del 17 novembre 1992, entrata in vigore il 1° maggio 1993 e successivamente modificata. Varie leggi settoriali hanno altresì recepito disposizioni in materia di tutela dei dati personali in molteplici settori come quelli della statistica, delle indagini di mercato, della ricerca scientifica e della sanità.

(7) L'Ungheria ha ratificato, con effetto dal 1° febbraio 1998, la convenzione del Consiglio d'Europa sulla protezione delle persone riguardo al trattamento automatizzato di dati di carattere personale (convenzione n. 108) [3], volta a rafforzare la tutela dei dati personali e ad assicurare la libera circolazione tra le parti contraenti, fatte salve le deroghe da queste eventualmente previste. Pur senza essere direttamente applicabile, la convenzione definisce gli obblighi internazionali per quanto riguarda non soltanto i principi fondamentali della protezione che ciascuna parte contraente deve attuare nel suo diritto interno, ma anche i meccanismi di cooperazione tra le parti contraenti. In particolare, le competenti autorità ungheresi devono fornire alle autorità delle altre parti contraenti che ne fanno richiesta ogni informazione sul diritto e sulle prassi amministrative in materia di protezione dei dati nonché informazioni relative ad ogni caso specifico di trattamento automatizzato di dati. Inoltre, esse devono prestare assistenza alle persone residenti all'estero nell'esercizio del loro diritto di essere informate

[1] GU L 281 del 23.11.1995, pag. 31.

[2] Parere 12/98, adottato dal gruppo di lavoro il 24 luglio 1998: «Trasferimento di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati» (DG MARKT D/5025/98), disponibile sul sito «Europa» della Commissione europea al seguente indirizzo: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

[3] http://conventions.coe.int/treaty/EN/cadreintro.htm.

circa l'esistenza di un trattamento di dati che le riguardano, del diritto di accedere ai dati che le riguardano e di chiederne la rettifica o la cancellazione, nonché del diritto di proporre un ricorso giurisdizionale.

(8) Le norme di legge vigenti in Ungheria incorporano tutti i principi fondamentali necessari per assicurare un livello di protezione adeguato delle persone fisiche, anche se eccezioni e limitazioni sono previste a salvaguardia di interessi pubblici rilevanti. L'applicazione di tali norme è garantita dai ricorsi giurisdizionali nonché dal controllo indipendente esercitato dal commissario nominato dal parlamento in forza della legge LXIII del 1992. Le legge garantisce inoltre il risarcimento delle persone che hanno subito un pregiudizio in conseguenza di un trattamento illecito.

(9) Nell'interesse della trasparenza e al fine di salvaguardare la capacità delle autorità competenti negli Stati membri di garantire la tutela delle persone fisiche per quanto concerne il trattamento dei dati personali che li riguardano, è necessario specificare nella decisione le circostanze eccezionali in cui, nonostante la constatazione di un livello di protezione adeguato, può essere giustificata la sospensione di trasferimenti di dati specifici.

(10) Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE si è pronunciato sul livello di protezione garantito dalla legislazione ungherese. In sede di elaborazione della presente decisione si è tenuto conto del parere espresso da tale gruppo [4].

(11) Le misure previste dalla presente decisione sono conformi al parere del comitato istituito dall'articolo 31 della direttiva 95/46/CE,

HA ADOTTATO LA PRESENTE DECISIONE:

*Articolo 1*

Ai fini dell'applicazione dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, per tutte le attività che rientrano nel campo d'applicazione della direttiva, si considera che l'Ungheria offra un livello adeguato di protezione dei dati personali trasferiti dall'Unione europea.

*Articolo 2*

La presente decisione riguarda soltanto l'adeguatezza della protezione garantita in Ungheria in base ai requisiti prescritti dall'articolo 25, paragrafo 1, della direttiva 95/46/CE e non incide su condizioni o restrizioni stabilite in applicazione di altre disposizioni della direttiva relativamente al trattamento di dati personali negli Stati membri.

*Articolo 3*

1. Fatta salva la loro facoltà di prendere provvedimenti per assicurare l'osservanza delle disposizioni nazionali adottate in conformità a disposizioni diverse da quelle di cui all'articolo 25 della direttiva 95/46/CE, le autorità competenti degli Stati membri possono esercitare i poteri di cui dispongono per sospendere trasferimenti di dati diretti ad un destinatario in Ungheria al fine di tutelare gli interessati in relazione al trattamento dei dati personali che li riguardano nei casi in cui:

a) la competente autorità ungherese abbia accertato che il destinatario viola le norme vigenti in materia di protezione, oppure

b) sia molto probabile una violazione delle norme di protezione; vi siano validi motivi per ritenere che la competente autorità ungherese non stia adottando o non adotterà misure adeguate e tempestive per risolvere il caso in questione; la continuazione del trasferimento comporti un rischio imminente di gravi danni per gli interessati e le autorità competenti degli Stati membri abbiano fatto il possibile, date le circostanze, per informare il soggetto stabilito in Ungheria che è responsabile del trattamento dei dati, dandogli la possibilità di replicare.

La sospensione cessa non appena sia garantito il rispetto delle norme di protezione e di ciò sia stata informata l'autorità competente della Comunità.

2. Gli Stati membri informano senza indugio la Commissione dell'adozione di misure in base al paragrafo 1.

3. Gli Stati membri e la Commissione si informano anche reciprocamente dei casi in cui le misure adottate dagli organismi incaricati di vigilare sul rispetto delle norme di protezione in Ungheria risultano inidonee a tal fine.

4. Se le informazioni raccolte in applicazione dei paragrafi 1, 2 e 3 del presente articolo dimostrano che uno degli organismi incaricati di vigilare sul rispetto delle norme di protezione in Ungheria non assolve efficacemente la sua funzione, la Commissione informa l'autorità ungherese competente e, se necessario, presenta un progetto delle misure da adottare secondo la procedura di cui all'articolo 31 della direttiva al fine di abrogare o sospendere la presente decisione o limitarne il campo d'applicazione.

[4] Parere 6/99, adottato dal gruppo di lavoro il 7 settembre 1999 (GD MARKT 5070/99), disponibile nel sito Web «Europa» della Commissione europea all'indirizzo indicato nella nota 2.

*Articolo 4*

1. La presente decisione può essere modificata in qualsiasi momento alla luce dell'esperienza acquisita nel corso della sua applicazione o di emendamenti apportati alla legislazione ungherese.

La Commissione valuta in ogni caso l'applicazione della presente decisione, sulla base delle informazioni disponibili, tre anni dopo la sua notifica agli Stati membri e riferisce ogni risultanza al comitato istituito a norma dell'articolo 31 della direttiva 95/46/CE, incluso ogni elemento che possa influire sulla valutazione di cui all'articolo 1 della presente decisione circa l'adeguatezza della protezione in Ungheria ai sensi dell'articolo 25 della direttiva 95/46/CE e ogni elemento da cui risulti che la decisione è applicata in modo discriminatorio.

2. La Commissione, se necessario, presenta un progetto delle misure da adottare conformemente alla procedura di cui all'articolo 31 della direttiva 95/46/CE.

*Articolo 5*

Gli Stati membri adottano le misure necessarie per conformarsi alla presente decisione entro novanta giorni dalla data della sua notifica agli Stati membri.

*Articolo 6*

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 26 luglio 2000.

*Per la Commissione*
Frederik BOLKESTEIN
*Membro della Commissione*

**01A11982**

GIANFRANCO TATOZZI, *direttore*

FRANCESCO NOCITA, *redattore*
ALFONSO ANDRIANI, *vice redattore*

(4651559/1) Roma, 2001 - Istituto Poligrafico e Zecca dello Stato - S.